JOURNAL OF ALGEBRA 42, 315–362 (1976)

A Characterization of the Galois Subbialgebras $H_k(K/F)$

MITSUHIRO TAKEUCHI

University of Tsukuba, Ibaraki, 300-31 Japan

Communicated by N. Jacobson

Received April 30, 1975

INTRODUCTION

Let K/k be an extension of fields of characteristic $p > 0$. Sweedler [6] defines a *pointed cocommutative k-bialgebra* $H_k(K)$ and a k-linear map $\omega: H_k(K) \otimes K \to K$ such that (i) ω *measures* K *to* K, i.e.,

$$\omega(a \otimes 1) = \epsilon(a)1 \qquad \text{and} \qquad \omega(a \otimes \lambda\mu) = \sum_{(a)} \omega(a_{(1)} \otimes \lambda)\, \omega(a_{(2)} \otimes \mu)$$

for $a \in H_k(K)$, $\lambda, \mu \in K$, (ii) K is a left $H_k(K)$-module through ω. The pair $(H_k(K), \omega)$ is characterized by some universality. We call $H_k(K)$ the *Galois* k-bialgebra of K/k.

When H is a *subbialgebra* of $H_k(K)$ put

$$K^H = \{\lambda \in K \mid \omega(a \otimes \lambda) = \epsilon(a)\lambda,\ \forall a \in H\},$$

which is a *subfield* of K containing k. Conversely if $K \supset F \supset k$ are fields, there is a unique maximal subbialgebra $H = H_k(K/F)$ such that $F \subset K^H$. We call $H_k(K/F)$ the *Galois* subbialgebra associated with F.

In order to establish the Galois correspondence between the set of intermediate fields $K \supset F \supset k$ and the set of subbialgebras H of $H_k(K)$:

$$F \mapsto H_k(K/F) \qquad \text{and} \qquad K^H \hookleftarrow H$$

we must solve the following two kinds of problems:

(i) to characterize the subfields F of the form K^H,

(ii) to characterize the Galois subbialgebras $H = H_k(K/F)$.

The first question was solved by Sweedler [6, Theorem 2.4] in case $[K:F] < \infty$: *If* $[K:F] < \infty$, *then* $F = K^H$ *for some subbialgebra* $H \subset H_k(K)$ *if and only if* (1) K *is normal over* F, *and* (2) F *and* kK^{p^n} *are linearly disjoint over* $F \cap kK^{p^n}$ *for all* n.

We solve the second problem in this paper, in case $[K:F] < \infty$ as well.

Let H be a subbialgebra of $H_k(K)$ and $F = K^H$. Let $K \# H$ denote the *smash product* k-algebra of K with H (0.7). Since K is naturally a *left* $K \# H$-module, we have a k-algebra map

$$\sigma: K \# H \to \mathrm{End}_F(K).$$

View $K \# H$ and $\mathrm{End}_F(K)$ as *left* K-modules. Then σ is K-linear. It is known (1.6.3) that $[K:F] < \infty$ if and only if $\sigma(K \# H)$ is finite dimensional as a left K-vector space.

Suppose $[K:F] < \infty$ in the following.

The k-algebra $K \# H$ together with the *K-coalgebra* structure $K \otimes H$, on which K acts on the left, becomes a *K/k-bialgebra* (1.4) (cf. [9] also) or a $\times_K$-bialgebra in terms of Sweedler [11].

Similarly the F-algebra $\mathrm{End}_F(K)$ together with the *dual K-coalgebra* structure $\mathrm{End}_F(K) = \mathsf{Mod}_K(K \otimes_F K, K)$ to the K-algebra $K \otimes_F K$, becomes a K/F-bialgebra and hence a K/k-bialgebra.

The K-linear map σ is a K-coalgebra map too, hence a map of K/k-bialgebras.

Let W_ℓ denote the category of *cocommutative* ℓ-coalgebras, for each field ℓ.

The scalar extension functor $K \otimes ?: \mathsf{W}_k \to \mathsf{W}_K$ has *the right adjoint functor* $\prod_{K/k} ?$, called *the Weil's restriction functor* (1.1). We denote by

$$\iota: C \to \prod_{K/k} (K \otimes C) \qquad \text{and} \qquad \gamma: K \otimes \prod_{K/k} \mathscr{C} \to \mathscr{C}$$

the *adjunctions*, for $C \in \mathsf{W}_k$ and $\mathscr{C} \in \mathsf{W}_K$.

In general if $\mathscr{H}$ is a cocommutative K/k-bialgebra, then there is a *unique* k-algebra structure on the k-coalgebra $\prod_{K/k} \mathscr{H}$ which makes it a k-bialgebra and the adjunction $\gamma: \prod_{K/k} \mathscr{H} \to \mathscr{H}$ into a k-algebra map (1.7.3).

Applying the functor $\prod_{K/k}$ to σ we obtain a map of k-bialgebras

$$\prod_{K/k} \sigma: \prod_{K/k} (K \# H) \to \prod_{K/k} \mathrm{End}_F(K).$$

Let $H^\#$ denote the *maximal pointed* subbialgebra of $\prod_{K/k} (K \# H)$. The maximal pointed subbialgebra of $\prod_{K/k} \mathrm{End}_F(K)$ is seen to equal $H_k(K/F)$ (1.8) by the universality. Hence $\prod_{K/k} \sigma$ induces a k-bialgebra map

$$\delta: H^\# \to H_k(K/F)$$

called *associated* with H. The composite $\delta \circ \iota: H \to H_k(K/F)$ with $\iota: H \to H^\#$ the adjunction, is the inclusion.

The purpose of this paper is to prove:

THEOREM 4.4. *Let H be a subbialgebra of $H_k(K)$. Then $H = H_k(K/F)$ for some subfield $K \supset F \supset k$ with $[K:F] < \infty$ if and only if* (1) $[\sigma(K \# H) : K] < \infty$ *and* (2) $\delta(H^*) \subset H$.

This theorem looks like Chase [2, Theorem 5.4], in which he assumes $[K : k] < \infty$ and K/F *purely inseparable modular* and uses $G_t(K/F/k)$ the *truncated k-group scheme* determined by $K/F/k$ instead of $H_k(K/F)$.

As a corollary we have a bijective Galois correspondence between the set of intermediate fields $K \supset F \supset k$ such that K/F is finite normal and F and kK^{p^n} are linearly disjoint for all n and the set of subbialgebras $H \subset H_k(K)$ such that $[\sigma(K \# H) : K] < \infty$ and $\delta(H^*) \subset H$ via $F \mapsto H_k(K/F)$ and $H \mapsto K^H$.

In Theorem 4.4, $H = H_k(K/F)$ does not follow from the condition (2) alone. We give a simple example of $H \subsetneqq hy_k(K) = H_k(K)^1$ with $k = K^H$ and $\delta(H^*) \subset H$, where $K = k(x, y)$ is purely transcendental over k.

In the Appendix we generalize the observation of Chase [2, Addendum] to the case when a *k-monoid functor* acts on a *k-functor*, and translate it into the language of coalgebras through the theory of *tangent coalgebras* [8] to obtain the above bialgebra structure on H^* and the bialgebra map δ. This will translate our main results into the language of the group schemers.

0. COALGEBRAS AND BIALGEBRAS OVER A FIELD

We recall some basic definitions and results on coalgebras and bialgebras over a field [4–7].

All rings and monoids are associative and have the unit. When R is a commutative ring, Mod_R denotes the category of R-modules. When A is a category and X, Y are objects of A, $\mathsf{A}(X, Y)$ denotes the set of A-morphisms from X to Y.

We fix a ground field k throughout the paper. When V and W are k-vector spaces, we write

$$V \otimes W = V \otimes_k W, \quad {}^tV = \mathsf{Mod}_k(V, k) \quad \text{and} \quad \langle X, x\rangle = \langle x, X\rangle = X(x)$$

for $X \in {}^tV$ and $x \in V$.

0.1. A *k-coalgebra* is a triple (C, Δ, ϵ) with $C \in \mathsf{Mod}_k$, $\Delta \in \mathsf{Mod}_k(C, C \otimes C)$ and $\epsilon \in \mathsf{Mod}_k(C, k)$ such that

$$(\Delta \otimes I) \circ \Delta = (I \otimes \Delta) \circ \Delta : C \to C \otimes C \otimes C,$$
$$(\epsilon \otimes I) \circ \Delta = I = (I \otimes \epsilon) \circ \Delta : C \to k \otimes C = C = C \otimes k.$$

We put for $c \in C$, $\Delta(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)}$. C is *cocommutative* if $\sum_{(c)} c_{(1)} \otimes c_{(2)} = \sum_{(c)} c_{(2)} \otimes c_{(1)}$ for all $c \in C$.

A subspace D of a k-coalgebra C is a ***subcoalgebra*** if $\Delta(D) \subset D \otimes D$. Then $(D, \Delta \mid D, \epsilon \mid D)$ is a k-coalgebra.

If $u: C \to D$ is a map of k-coalgebras, of which the definition is obvious, then $u(C)$ is a subcoalgebra of D.

A k-coalgebra is the union of its *finite dimensional* subcoalgebras [7, Sect. 2.2].

If C and D are k-coalgebras, the tensor product $C \otimes D$ is a k-coalgebra by

$$\Delta(c \otimes d) = \sum_{(c,d)} c_{(1)} \otimes d_{(1)} \otimes c_{(2)} \otimes d_{(2)}, \qquad \epsilon(c \otimes d) = \epsilon(c)\,\epsilon(d)$$

for $c \in C$, $d \in D$.

If ℓ/k is an extension of fields, then $\ell \otimes C$ is obviously an ℓ-coalgebra for each k-coalgebra C.

We denote by W_k the category of *cocommutative* k-coalgebras. The tensor product $C \otimes D$ is the product in W_k. The coalgebra k is a final object.

A *k-bialgebra* is a k-coalgebra (H, Δ, ϵ) where H is a k-algebra and $\Delta: H \to H \otimes H$, $\epsilon: H \to k$ are k-algebra maps. Morphisms of k-bialgebras are obviously defined.

A subspace L of a k-bialgebra H is a ***subbialgebra*** if it is a subalgebra and a subcoalgebra of H. L is then a k-bialgebra. If $u: L \to H$ is a map of k-bialgebras, then $u(L)$ is a subbialgebra of H.

If L and H are k-bialgebras, then the tensor product $L \otimes H$ is a k-bialgebra with the tensor product algebra and coalgebra structure.

If ℓ/k is a field extension, then $\ell \otimes H$ is an ℓ-bialgebra for each k-bialgebra H.

A *cocommutative* k-bialgebra H is by definition a *monoid object* in the category W_k. Hence, the set $\mathsf{W}_k(C, H)$ is a monoid for all $C \in \mathsf{W}_k$.

0.2. If A is a k-algebra and C a k-coalgebra, then the k-space $\mathsf{Mod}_k(C, A)$ is a k-algebra with the *convolution product*

$$f * g = \mu \circ (f \otimes g) \circ \Delta, \qquad f, g \in \mathsf{Mod}_k(C, A)$$

and with the unit $\eta \circ \epsilon$, where (μ, η) denotes the algebra structure on A ($\mu: A \otimes A \to A$, $\eta: k \to A$). In particular the dual space ${}^tC = \mathsf{Mod}_k(C, k)$ is a k-algebra.

If H is a cocommutative k-bialgebra, then the monoid $\mathsf{W}_k(C, H)$ is a multiplicative submonoid of the algebra $\mathsf{Mod}_k(C, H)$ for $C \in \mathsf{W}_k$.

If A is a *finite dimensional* k-algebra, then the dual space ${}^tA$ has a natural k-coalgebra structure.

0.3. Let C be a k-coalgebra.

C is *simple if* $C \neq 0$ and has no proper subcoalgebras.

C is *irreducible* if $C \neq 0$ and any two nonzero subcoalgebras of C have nonzero intersection.

C is *pointed* if every simple subcoalgebra of C is one-dimensional.

C is *connected* if it is pointed and irreducible.

A maximal irreducible subcoalgebra of C is called an *irreducible component* of C.

Let $G(C) = \{x \in C \mid \Delta(x) = x \otimes x \text{ and } \epsilon(x) = 1\}$ (the set of *group-like* elements in C) identified with the set of coalgebra maps from k to C. For $g \in G(C)$, C^g denotes the irreducible component of C containing g.

If ℓ/k is an extension of fields and $g \in G(C)$, then by [7, 11.0.8]

$$(\ell \otimes C)^g = \ell \otimes C^g.$$

If C is a connected k-coalgebra, $G(C)$ consists of only one element, which we shall denote by 1. If $u: C \to D$ is a k-coalgebra map where C is connected, then $u(C)$ is connected and contained in $D^{u(1)}$.

If H is a k-bialgebra, then the unit 1 is in $G(H)$. The irreducible component H^1 is a subbialgebra [7, Sect. 8.1].

A connected cocommutative k-bialgebra is called a *k-hyperalgebra.* Any subbialgebra of a k-hyperalgebra is also a k-hyperalgebra, called a *subhyperalgebra.*

If $u: L \to H$ is a map of k-bialgebras with L a k-hyperalgebra, then $u(L)$ is a k-hyperalgebra contained in H^1.

The tensor product of two k-hyperalgebras is a k-hyperalgebra.

If ℓ/k is a field extension, then $\ell \otimes H$ is an ℓ-hyperalgebra when H is a k-hyperalgebra.

0.4. Let B_k denote the k-coalgebra on a free basis $\{b_0, b_1, \ldots\}$ with the structure

$$\Delta(b_n) = \sum_{i=0}^{n} b_i \otimes b_{n-i}, \qquad \epsilon(b_n) = \delta_{n,0}.$$

B_k is connected cocommutative. The subspaces

$$B_{k,n} = kb_0 + kb_1 + \cdots + kb_n$$

are subcoalgebras of B_k.

Let C be a k-coalgebra. For each $g \in G(C)$ put

$$P_g(C) = \{x \in C \mid \Delta(x) = x \otimes g + g \otimes x\}.$$

If ℓ/k is a field extension, then $P_g(\ell \otimes C) = \ell \otimes P_g(C)$.

A map of k-coalgebras $\phi: B_k \to C$ (resp. $\phi: B_{k,n} \to C$) is called an *∞-sequence* (resp. an *n-sequence*) *of divided powers* (or SDP) in C. This can be identified with a sequence $\{c_0, c_1, \ldots\}$ (resp. $\{c_0, c_1, \ldots, c_n\}$) of elements in C with

$$\Delta(c_j) = \sum_{i=0}^{j} c_i \otimes c_{j-i}, \qquad \epsilon(c_j) = \delta_{j,0}.$$

The set of 1-SDP's in C is identified with the disjoint union

$$\coprod_{g \in G(C)} P_g(C).$$

If C is connected, we put $P(C) = P_1(C)$. A map of k-coalgebras $u: C \to D$ with C connected is injective if so is the restriction $u \mid P(C)$ [7, Sect. 11.0].

When H is a k-bialgebra, we put $P(H) = P_1(H)$ which is a (p-) Lie subalgebra of H (if the characteristic of k is $p > 0$).

0.5. Each k-coalgebra C has a natural filtration

$$C_0 \subset C_1 \subset C_2 \subset \cdots$$

called the *coradical filtration*, which satisfies the following properties [7, Sect. 9.1]:

$$C = \bigcup_n C_n , \tag{0.5.1}$$

$$\Delta(C_n) \subset \sum_{i=0}^{n} C_i \otimes C_{n-i} , \tag{0.5.2}$$

0.5.3. C_0 is the sum of simple subcoalgebras of C.

Let $C^+ = \mathrm{Ker}(\epsilon: C \to k)$ and $C_n{}^+ = C^+ \cap C_n$.

0.5.4. If C is connected, then $C_0 = k1$ and $C_1 = k1 \oplus P(C)$. For each $x \in C_n{}^+$, $\Delta(x) - x \otimes 1 - 1 \otimes x \in \sum_{i=0}^{n} C_i{}^+ \otimes C_{n-i}^+ \subset C_{n-1}^+ \otimes C_{n-1}^+$ [7, Proposition 10.0.2]. If ℓ/k is a field extension, then $(\ell \otimes C)_n = \ell \otimes C_n$ [4, I, 3.2.3].

The coradical filtration on B_k (0.4) is given by $\{B_{k,n}\}_{n=0}^{\infty}$.

0.6. For each k-vector space V, there are a *cocommutative* k-coalgebra $C_k(V)$ and a k-linear map $\pi: C_k(V) \to V$ satisfying the UMP: For all $C \in \mathsf{W}_k$, the map

$$\mathsf{W}_k(C, C_k(V)) \to \mathsf{Mod}_k(C, V), \qquad \phi \mapsto \pi \circ \phi$$

is *bijective*. The pair $(C_k(V), \pi)$ (uniquely determined) is called the *cofree cocommutative* k-coalgebra on V with π the canonical map [7, Sect. 6.4].

Let $\mu: C_k(V) \otimes C_k(V) \to C_k(V)$ and $\eta: k \to C_k(V)$ be the k-coalgebra maps defined by

$$\pi \circ \mu = \pi \otimes \epsilon + \epsilon \otimes \pi: C_k(V) \otimes C_k(V) \to V,$$
$$\pi \circ \eta = 0: k \to V.$$

The coalgebra $C_k(V)$ is a commutative k-bialgebra with the algebra structure (μ, η) [7, Theorem 6.4.8].

We denote by $B_k(V)$ the irreducible component $C_k(V)^1$ which is a k-hyperalgebra. The restriction $\pi: B_k(V) \to V$ satisfies the UMP: For all $C \in \mathsf{W}_k$ *connected*, the map

$$\mathsf{W}_k(C, B_k(V)) \to \mathsf{Mod}_k(C^+, V), \qquad \phi \mapsto \pi \circ \phi \mid C^+$$

is *bijective* [7, Theorem 12.2.5].

The structure theorem of $B_k(V)$ [7, Theorem 12.3.2] implies that if ℓ/k is a field extension, then $\ell \otimes B_k(V) \simeq B_\ell(\ell \otimes V)$.

We have $B_k = B_k(k)$ (0.4). The algebra structure is given by

$$b_i b_j = \binom{i+j}{i} b_{i+j} \qquad \text{and} \qquad b_0 = 1.$$

0.7. Let A and B be k-algebras, C a k-coalgebra and $\omega: C \otimes A \to B$ a k-linear map. We say that ω *measures A to B* [7, Sect. 7.0] if

$$\omega(c \otimes 1) = \epsilon(c)1 \qquad \text{and} \qquad \omega(c \otimes xy) = \sum_{(c)} \omega(c_{(1)} \otimes x)\, \omega(c_{(2)} \otimes y)$$

for all $c \in C$, $x, y \in A$ or equivalently if the k-linear map

$$A \to \mathsf{Mod}_k(C, B), \qquad x \mapsto \omega(\,? \otimes x)$$

is a k-algebra map.

There is a *cocommutative* k-coalgebra $M_k(A, B)$ which measures A to B by $\Phi: M_k(A, B) \otimes A \to B$ satisfying the UMP: For each $C \in \mathsf{W}_k$ and a measuring $\omega: C \otimes A \to B$, there is a unique map $u \in \mathsf{W}_k(C, M_k(A, B))$ with $\omega = \Phi \circ (u \otimes A)$ [7, Theorem 7.0.4].

Let H be a k-bialgebra. We say that A is a left *H-module algebra* [7, Sect. 7.2] if A is a left H-module such that the structure map

$$H \otimes A \to A, \qquad a \otimes \lambda \mapsto a[\lambda]$$

measures A to A. The *smash product* k-algebra $A \# H$ is defined as follows [7, Sect. 7.2]: $A \# H = A \otimes H$ as a k-space. We write $\lambda \# a = \lambda \otimes a$ for $\lambda \in A$, $a \in H$. The multiplication is defined by

$$(\lambda \# a)(\mu \# b) = \sum_{(a)} \lambda \cdot a_{(1)}[\mu] \# a_{(2)} b.$$

The unit is $1 \# 1$.

We put $M_k(A) = M_k(A, A)$. This has a *unique* k-bialgebra structure such that $\Phi: M_k(A) \otimes A \to A$ is a left module structure [7, Sect. 7.0].

If H is a k-bialgebra, a k-algebra map $\rho: H \to \mathrm{End}_k(A)$ is called a *measuring representation* if it makes A into a left H-module algebra. The bialgebra $M_k(A)$ has the canonical measuring representation $\Theta: M_k(A) \to \mathrm{End}_k(A)$.

Each measuring representation $\rho: H \to \mathrm{End}_k(A)$ factors as $\rho = \Theta \circ u$ with a unique bialgebra map $u: H \to M_k(A)$ if H is *cocommutative*.

For each subcoalgebra C of $M_k(A)$ put

$$A^C = \{x \in A \mid \Phi(c \otimes x) = \epsilon(c)x, \forall c \in C\},$$

which is a subalgebra of A. If A is a *field* then A^C is a *subfield* [7, Sect. 10.1].

For each subalgebra F of A, there is a ***unique maximal*** subcoalgebra C of $M_k(A)$ such that $F \subset A^C$. We put $C = M_k(A/F)$ which is a *subbialgebra* of $M_k(A)$.

We put $hy_k(A) = M_k(A)^1$ and $hy_k(A/F) = M_k(A/F)^1$ the irreducible components, which are k-hyperalgebras.

The canonical measuring $\Phi: hy_k(A) \otimes A \to A$ has the UMP: Let $C \in \mathsf{W}_k$ be *connected* and $\omega: C \otimes A \to A$ a measuring such that $\omega(1 \otimes a) = a$, $\forall a \in A$. There is a unique map $u \in \mathsf{W}_k(C, hy_k(A))$ such that $\Phi \circ (u \otimes A) = \omega$. The image $u(C)$ is contained in $hy_k(A/F)$ if and only if the maps $\omega(c \otimes ?)$: $A \to A$ are left (or right) F-linear.

If $\rho: H \to \mathrm{End}_k(A)$ is a measuring representation of a *k-hyperalgebra* H, then ρ factors as $\rho = \Theta \circ u$ with a unique hyperalgebra map $u: H \to hy_k(A)$ where $\Theta: hy_k(A) \to \mathrm{End}_k(A)$ is the canonical measuring representation.

Let $\mathrm{Der}_k(A)$ denote the k-Lie algebra of *k-linear derivations* of A into A. For a subalgebra F of A, put

$$\mathrm{Der}_k(A/F) = \{d \in \mathrm{Der}_k(A) \mid d(\lambda) = 0, \forall \lambda \in F\},$$

which is a Lie subalgebra.

By [7, Sect. 7.2, Ex. 3)] we have $P(hy_k(A/F)) \simeq \mathrm{Der}_k(A/F)$ as (*restricted*) *k-Lie algebras*.

0.8. Let the characteristic of k be $p > 0$. In the algebraic closure $\bar{k}$ of k we put $k^{-i} = \{x \in \bar{k} \mid x^{p^i} \in k\}$.

If V (resp. W) is a k- (resp. k^{-i}-) vector space, a homomorphism of abelian groups $u: V \to W$ is *p^{-i}-linear* if

$$u(\lambda v) = \lambda^{p^{-i}} \cdot u(v), \qquad \forall \lambda \in k,\ v \in V.$$

When ℓ/k is a field extension, we view $\ell \supset \bar{k}$, hence $\ell^{-i} \supset k^{-i}$ for all i. If $u: V \to W$ is a p^{-i}-linear map with V, W as above, the p^{-i}-linear map $\bar{u}: \ell \otimes V \to \ell^{-i} \otimes_{k^{-i}} W$, $\lambda \otimes v \mapsto \lambda^{p^{-i}} \otimes u(v)$ is well defined.

Let $C \in \mathsf{W}_k$. There is a unique p^{-1}-linear map

$$\mathscr{V}: C \to k^{-1} \otimes C$$

such that $\langle \mathscr{V}(c), \lambda \otimes X \rangle^p = \langle c, \lambda^p X^p \rangle$ for $c \in C$, $\lambda \in k^{-1}$ and $X \in {}^tC$ [4, II, 4.1.8]. Iterating the $\mathscr{V}$-map we put

$$\mathscr{V}^n: C \to k^{-n} \otimes C.$$

The image $\mathscr{V}^n(C)$ is a k^{-n}-subcoalgebra of $k^{-n} \otimes C$ and if H is a cocommutative k-bialgebra, then $\mathscr{V}^n(H)$ is a k^{-n}-subbialgebra of $k^{-n} \otimes H$ [4, II, 4.1.6].

If $u: C \to D$ is a W_k-map, then $\mathscr{V}_D{}^n \circ u = [k^{-n} \otimes u] \circ \mathscr{V}_C{}^n: C \to k^{-n} \otimes D$ [4, II, 4.1.5].

By definition, the $\mathscr{V}^n$-map of the ℓ-coalgebra $\ell \otimes C$ is obtained from $\mathscr{V}^n: C \to k^{-n} \otimes C$ by the scalar extension

$$\overline{\mathscr{V}^n}: \ell \otimes C \to \ell^{-n} \otimes_{k^{-n}} (k^{-n} \otimes C) = \ell^{-n} \otimes_{\ell} (\ell \otimes C).$$

Suppose k is perfect. Then $k^{-i} = k$ for all i. Let H be a k-hyperalgebra. Then $\mathscr{V}^n(H)$ are subhyperalgebras of H. Hence $P(\mathscr{V}^n(H)) = \mathscr{V}^n(H) \cap P(H)$ are p-Lie subalgebras of $P(H)$.

0.8.1. THEOREM. [5, Theorem 2] *Let H be a hyperalgebra over a perfect field of characteristic $p > 0$. A primitive element $x \in P(H)$ is in $\mathscr{V}^n(H)$ if and only if there is a $(p^{n+1} - 1)$-SDP in H lying over x.*

The following is a direct consequence of [4, II, Lemma 4.2.5]:

0.8.2. LEMMA. *If H is a hyperalgebra over a field of characteristic $p > 0$, then the coradical filtration on $\mathscr{V}(H)$ is given by*

$$\mathscr{V}(H)_n = \mathscr{V}(H) \cap H_n = \mathscr{V}(H_{np}).$$

Hence inductively

$$\mathscr{V}^r(H)_n = \mathscr{V}^r(H) \cap H_n = \mathscr{V}^r(H_{np^r}).$$

0.9. We assume k is a field. But some of the definitions make sense and some of the results hold true as they stand when k is a *commutative ring* too. For example the following concepts are meaningful over a commutative ring k:

> coalgebra, cocommutative, W_k, bialgebra, the tensor product of coalgebras or bialgebras, the scalar extension $\ell \otimes C$ or $\ell \otimes H$, the algebras $\mathsf{Mod}_k(C, A)$ and ${}^tC$, the coalgebra ${}^tA$ when A is a *finite projective* k-algebra, $G(C)$, B_k, $B_{k,n}$, $P_g(C)$, ∞- or n-SDP, measuring, module algebra, smash product, A^C.

But we consider the following concepts only when k is a field (cf. [10]):

> subcoalgebra, subbialgebra, simple, irreducible, connected, C^g, hyperalgebra, coradical filtration, $C_k(V)$, $B_k(V)$, $M_k(A, B)$, $hy_k(A)$, the $\mathscr{V}$-map.

The reader can easily check which facts on coalgebras or bialgebras are valid over a commutative ring.

For example [7, Lemma 11.0.1] (0.4) can be extended as follows:

0.9.1. PROPOSITION. *Let K be a commutative k-algebra with k a field. Let C be a connected k-coalgebra, $\mathscr{C}$ a K-coalgebra and*

$$\phi: K \otimes C \to \mathscr{C}$$

a K-coalgebra map. Suppose $\mathscr{C}$ is a flat K-module. If $\phi \mid K \otimes P(C)$ is injective then the map ϕ is injective.

Proof is similar to [7, Lemma 11.0.1]. We can prove the injectivity of $\phi \mid K \otimes C_n^+$ by induction based on (0.5.4). We use the fact $K \otimes P(C) = P(K \otimes C)$. The flatness is used to show that the injectivity of $\phi \mid K \otimes C_n^+$ implies that of

$$\phi \otimes_K \phi: K \otimes C_n^+ \otimes C_n^+ \to \mathscr{C} \otimes_K \mathscr{C}.$$

1. WEIL'S RESTRICTION FUNCTOR AND K/k-BIALGEBRAS

We fix a field k, a commutative k-algebra K, an extension field ℓ/k and a subalgebra F of K. We put $\tilde{K} = \ell \otimes K$ and $\tilde{F} = \ell \otimes F$.

1.1. Recall that W_K denotes the category of cocommutative K-coalgebras (0.9). If $C \in \mathsf{W}_k$, then $K \otimes C \in \mathsf{W}_K$.

PROPOSITION–DEFINITION. *The scalar extension $K \otimes ?: \mathsf{W}_k \to \mathsf{W}_K$ has the right adjoint functor which is denoted by $\prod_{K/k}$ and called the Weil's restriction functor.*

Proof. Let $\mathscr{C} \in \mathsf{W}_K$. Let $C_k(\mathscr{C})$ denote the cofree cocommutative k-coalgebra on the k-space $\mathscr{C}$ (0.6). Let $\mathscr{X}$ denote the set of subcoalgebras D of $C_k(\mathscr{C})$ such that the K-linear map

$$K \otimes D \to \mathscr{C}, \qquad \lambda \otimes c \mapsto \lambda \cdot \pi(c)$$

with $\pi: C_k(\mathscr{C}) \to \mathscr{C}$ the canonical map, is a K-coalgebra map. The sum $\prod_{K/k} \mathscr{C} = \sum_{D \in \mathscr{X}} D$ is clearly the largest element of $\mathscr{X}$ and we have naturally

$$\mathsf{W}_k\left(C, \prod_{K/k} \mathscr{C}\right) \simeq \mathsf{W}_K(K \otimes C, \mathscr{C}), \qquad \forall C \in \mathsf{W}_k. \qquad \text{Q.E.D.}$$

1.1.1. We denote by

$$\iota: C \to \prod_{K/k} (K \otimes C) \qquad \text{and} \qquad \gamma: K \otimes \prod_{K/k} \mathscr{C} \to \mathscr{C}$$

the *adjunctions* for $C \in \mathsf{W}_k$ and $\mathscr{C} \in \mathsf{W}_K$.

1.2. For each $C \in \mathsf{W}_k$ (resp. $\mathscr{C} \in \mathsf{W}_K$), we can view $\ell \otimes C \in \mathsf{W}_\ell$ (resp. $\ell \otimes \mathscr{C} \in \mathsf{W}_K$) in an obvious manner.

THEOREM. *Suppose the extension ℓ/k is algebraic. For all $\mathscr{C} \in \mathsf{W}_K$,*

$$\ell \otimes \left(\prod_{K/k} \mathscr{C} \right) \simeq \prod_{K/\ell} (\ell \otimes \mathscr{C}) \qquad \text{in} \quad \mathsf{W}_\ell .$$

Proof. Case $[\ell : k] < \infty$. The dual k-space ${}^t\ell$ is a cocommutative k-coalgebra (0.2) and an ℓ-vector space through

$$\langle \lambda x, \mu \rangle = \langle x, \lambda\mu \rangle \qquad \text{for} \quad \lambda, \mu \in \ell, \quad x \in {}^t\ell.$$

The comultiplication $\Delta: {}^t\ell \to {}^t\ell \otimes {}^t\ell$ satisfies

$$\Delta(\lambda x) = \sum_{(x)} \lambda x_{(1)} \otimes x_{(2)} = \sum_{(x)} x_{(1)} \otimes \lambda x_{(2)}$$

for $x \in {}^t\ell$ and $\lambda \in \ell$. For ℓ-vector spaces V and W, the k-linear map

$$\alpha(V, W): {}^t\ell \otimes_\ell V \otimes_\ell W \to ({}^t\ell \otimes_\ell V) \otimes ({}^t\ell \otimes_\ell W),$$
$$x \otimes_\ell v \otimes_\ell w \mapsto \sum_{(x)} (x_{(1)} \otimes_\ell v) \otimes (x_{(2)} \otimes_\ell w)$$

is hence well defined. For each $C \in \mathsf{W}_\ell$, the structure maps

$$\tilde{\Delta}: {}^t\ell \otimes_\ell C \xrightarrow{{}^t\ell \otimes_\ell \Delta} {}^t\ell \otimes_\ell C \otimes_\ell C \xrightarrow{\alpha(C,C)} ({}^t\ell \otimes_\ell C) \otimes ({}^t\ell \otimes_\ell C),$$
$$\tilde{\epsilon}: {}^t\ell \otimes_\ell C \xrightarrow{{}^t\ell \otimes_\ell \epsilon} {}^t\ell \otimes_\ell \ell = {}^t\ell \xrightarrow{\langle ?, 1 \rangle} k$$

make ${}^t\ell \otimes_\ell C$ into a cocommutative k-coalgebra.

Note that for an ℓ-vector space V and a k-vector space W we have $\mathsf{Mod}_\ell(V, \ell \otimes W) \simeq \mathsf{Mod}_k({}^t\ell \otimes_\ell V, W)$ naturally. It is easy to check that this induces

$$\mathsf{W}_\ell(C, \ell \otimes D) \simeq \mathsf{W}_k({}^t\ell \otimes_\ell C, D)$$

for all $C \in \mathsf{W}_\ell$ and $D \in \mathsf{W}_k$.

Now let $C \in \mathbf{W}_\ell$ and $\mathscr{C} \in \mathbf{W}_K$. Then

$$\mathbf{W}_\ell\left(C, \ell \otimes \prod_{K/k} \mathscr{C}\right) \simeq \mathbf{W}_k\left({}^t\ell \otimes_\ell C, \prod_{K/k} \mathscr{C}\right)$$

$$\simeq \mathbf{W}_K(K \otimes {}^t\ell \otimes_\ell C, \mathscr{C}) \simeq \mathbf{W}_K\left([K \otimes {}^t\ell] \underset{[K\otimes\ell]}{\otimes} [K \otimes C], \mathscr{C}\right)$$

$$\overset{(*)}{\simeq} \mathbf{W}_{K\otimes\ell}(K \otimes C, [K \otimes \ell] \otimes_K \mathscr{C}) \simeq \mathbf{W}_{\tilde{K}}(\tilde{K} \otimes_\ell C, \ell \otimes \mathscr{C})$$

$$\simeq \mathbf{W}_\ell\left(C, \prod_{\tilde{K}/\ell} (\ell \otimes \mathscr{C})\right),$$

where the isomorphism $(*)$ holds, because $\ell \otimes K$ is a finite projective K-module and the above arguments are valid for ℓ/k replaced with $\tilde{K}/K$. This chain of isomorphisms shows that

$$\ell \otimes \left(\prod_{K/k} \mathscr{C}\right) \simeq \prod_{\tilde{K}/\ell} (\ell \otimes \mathscr{C}).$$

Case ℓ/k is algebraic. The adjunction

$$\gamma\colon K \otimes \prod_{K/k} \mathscr{C} \to \mathscr{C}$$

induces a natural map

$$\mathbf{W}_\ell\left(C, \ell \otimes \prod_{K/k} \mathscr{C}\right) \to \mathbf{W}_{\tilde{K}}(K \otimes C, \ell \otimes \mathscr{C})$$

for all $C \in \mathbf{W}_\ell$, $\mathscr{C} \in \mathbf{W}_K$. We have shown above that this is an isomorphism when $[\ell : k] < \infty$. To generalize this to the case ℓ/k is algebraic, we can assume $[C : \ell] < \infty$, since an arbitrary ℓ-coalgebra is the union of finite dimensional subcoalgebras (0.1). Let $\{x_1, \ldots, x_n\}$ be an ℓ-basis for C with

$$\Delta(x_i) = \sum_{j,k} \xi_{ijk} x_j \otimes x_k,$$

where $\xi_{ijk} \in \ell$. Let $\phi \in \mathbf{W}_{\tilde{K}}(K \otimes C, \ell \otimes \mathscr{C})$. There is an intermediate field $k \subset \ell' \subset \ell$ such that $\xi_{ijk} \in \ell'$, $\epsilon(x_i) \in \ell'$, $\phi(x_i) \in \ell' \otimes \mathscr{C}$ for all i, j, k and $[\ell' : k] < \infty$. Then

$$C' = \ell' x_1 + \cdots + \ell' x_n$$

is a cocommutative ℓ'-coalgebra and we can view

$$\phi\colon K \otimes C' \to \ell' \otimes \mathscr{C}$$

as an $\ell' \otimes K$-coalgebra map. Since $[\ell' : k] < \infty$, ϕ comes from some $\mathbf{W}_{\ell'}$-morphism: $C' \to \ell' \otimes \prod_{K/k} \mathscr{C}$. Applying the scalar extension $\ell \otimes_{\ell'} ?$, we conclude the surjectivity of the natural map: $\mathbf{W}_\ell(C, \ell \otimes \prod_{K/k} \mathscr{C}) \to \mathbf{W}_{\tilde{K}}(K \otimes C, \ell \otimes \mathscr{C})$. The injectivity can be proved similarly. Q.E.D.

1.2.1. *Remark.* The above theorem implies that if $C \in \mathbf{W}_k$ and $\mathscr{C} \in \mathbf{W}_K$, then

$$\ell \otimes \iota\colon \ell \otimes C \to \ell \otimes \prod_{K/k} (K \otimes C) = \prod_{\tilde{K}/\ell} [\tilde{K} \otimes_\ell (\ell \otimes C)],$$

$$\ell \otimes \gamma\colon \ell \otimes K \otimes \prod_{K/k} \mathscr{C} = \tilde{K} \otimes_\ell \prod_{\tilde{K}/\ell} (\ell \otimes \mathscr{C}) \to \ell \otimes \mathscr{C}$$

are the *adjunctions*.

1.3. Let $\mathscr{C} \in \mathbf{W}_K$. The sets of group-like elements $G(\mathscr{C})$ and $G(\prod_{K/k} \mathscr{C})$ can be identified with each other, since

$$G(\mathscr{C}) = \mathbf{W}_K(K, \mathscr{C}) = \mathbf{W}_k\left(k, \prod_{K/k} \mathscr{C}\right) = G\left(\prod_{K/k} \mathscr{C}\right).$$

Since $B_K = K \otimes B_k$ and $B_{K,n} = K \otimes B_{k,n}$, we have similarly

$$\mathbf{W}_K(B_K, \mathscr{C}) \simeq \mathbf{W}_k\left(B_k, \prod_{K/k} \mathscr{C}\right), \quad \mathbf{W}_K(B_{K,n}, \mathscr{C}) \simeq \mathbf{W}_k\left(B_{k,n}, \prod_{K/k} \mathscr{C}\right),$$

which show that the set of ∞- (resp. n-) SDP's in $\mathscr{C}$ can be canonically identified with the set of those sequences in $\prod_{K/k} \mathscr{C}$.

Since $\mathbf{W}_K(B_{K,1}, \mathscr{C}) \simeq \coprod_{g \in G(\mathscr{C})} P_g(\mathscr{C})$ (0.4), it follows that

$$P_g(\mathscr{C}) \simeq P_g\left(\prod_{K/k} \mathscr{C}\right)$$

for all $g \in G(\mathscr{C}) = G(\prod_{K/k} \mathscr{C})$. This can be shown to be an isomorphism of *k-spaces* (cf. [3, II, Sect. 4] or [8, 1, Sect. 3b]). In particular the k-space $P_g(\prod_{K/k} \mathscr{C})$ has a natural structure of *K-module.*

1.4. *K/k-Bialgebras.* We view each K-coalgebra as a *left* K-module. A *K/k-bialgebra* [9, 1.7] is a K-coalgebra $\mathscr{H}$ together with a k-algebra structure such that

1. $(\lambda a)b = \lambda(ab)$,
2. $\sum_{(a)} a_{(1)}\lambda \otimes_K a_{(2)} = \sum_{(a)} a_{(1)} \otimes_K a_{(2)}\lambda$ in $\mathscr{H} \otimes_K \mathscr{H}$,
3. $\Delta(1) = 1 \otimes_K 1$ in $\mathscr{H} \otimes_K \mathscr{H}$,
4. $\Delta(ab) = \Delta(a)\,\Delta(b)$ in $\mathscr{H} \otimes_K \mathscr{H}$,
5. $\epsilon(ab) = \epsilon(a\epsilon(b))$,
6. $\epsilon(1) = 1$

for all $\lambda \in K$ and $a, b \in \mathscr{H}$. In 2, 3, and 4, $\mathscr{H} \otimes_K \mathscr{H}$ is the tensor product of two copies of the *left* K-module $\mathscr{H}$. Condition 1 implies that $K \to \mathscr{H}$, $\lambda \mapsto \lambda 1$ is a k-algebra map from which the left K-module structure on $\mathscr{H}$ comes, i.e., $\lambda a = (\lambda 1)a$ for $\lambda \in K$ and $a \in \mathscr{H}$. Hence $\mathscr{H}$ has a *right* K-module structure

$$a\lambda = a(\lambda 1) \qquad \text{for} \quad \lambda \in K \quad \text{and} \quad a \in \mathscr{H}.$$

In 2 and 5, the elements $a\lambda$ or $a\epsilon(b)$ are in this sense. Since we have $(a\lambda)b = a(\lambda b)$ for $\lambda \in K$ and $a, b \in \mathscr{H}$, it follows from 2 that the k-linear map

$$u \otimes_K v \mapsto \sum_{(a)} a_{(1)}u \otimes_K a_{(2)}v, \ \mathscr{H} \otimes_K \mathscr{H} \to \mathscr{H} \otimes_K \mathscr{H}$$

is well defined for all $a \in \mathscr{H}$. In particular the product $\Delta(a)\,\Delta(b)$ in 4 makes sense.

A K/k-bialgebra is a $\times_K$-*bialgebra* over k [11, 5.6, p. 108] if the underlying K-bimodule is *associative* [11, 2.7, p. 95]. In particular if K is a *field*, the K/k-bialgebras are the same as the $\times_K$-bialgebras by [11, 2.5, p. 93].

A k/k-bialgebra is the same as a *k-bialgebra* (0.1).

A K-linear map $\phi: \mathscr{L} \to \mathscr{H}$ of K/k-bialgebras is a homomorphism if it is a K-coalgebra map and a k-algebra map.

1.4.1. Let $\mathscr{C}$ be a K-coalgebra. A left K-linear map $\omega: \mathscr{C} \otimes K \to K$ (the left K-module structure on $\mathscr{C} \otimes K$ induced from that on $\mathscr{C}$) is called to *measure K to K*, if

$$\omega(a \otimes \lambda\mu) = \sum_{(a)} \omega(a_{(1)} \otimes \lambda)\,\omega(a_{(2)} \otimes \mu),$$

$$\omega(a \otimes 1) = \epsilon(a)$$

for $a \in \mathscr{C}$ and $\lambda, \mu \in K$. Note that the element $\sum_{(a)} \omega(a_{(1)} \otimes \lambda)\,\omega(a_{(2)} \otimes \mu)$ is well defined, since ω is left K-linear. It is easy to see that ω measures K to K if and only if the k-linear map

$$K \to \mathsf{Mod}_K(\mathscr{C}, K), \qquad \lambda \mapsto \omega(\,? \otimes \lambda)$$

is a *k-algebra* map (cf. (0.2), (0.9), (0.7)).

PROPOSITION. *Let $\mathscr{H}$ be a K/k-bialgebra. Then $a[\lambda] =_{\text{def}} \epsilon(a\lambda)$ for $a \in \mathscr{H}$ and $\lambda \in K$ measures K to K and makes K into a left $\mathscr{H}$-module.*

Proof. Let $a, b \in \mathscr{H}$ and $\lambda, \mu \in K$. The map $a \mapsto a[\lambda]$ is left K-linear. We have $a[1] = \epsilon(a1) = \epsilon(a)$. Since

$$\Delta(a\lambda) = \sum_{(a)} a_{(1)}\lambda \otimes_K a_{(2)}\,,$$

we have $a\lambda = \sum_{(a)} \epsilon(a_{(1)}\lambda)\, a_{(2)} = \sum_{(a)} a_{(1)}[\lambda]\, a_{(2)}$, $a\lambda\mu = \sum_{(a)} a_{(1)}[\lambda]\, a_{(2)}\mu$ and hence

$$a[\lambda\mu] = \epsilon(a\lambda\mu) = \sum_{(a)} a_{(1)}[\lambda]\, \epsilon(a_{(2)}\mu) = \sum_{(a)} a_{(1)}[\lambda]\, a_{(2)}[\mu].$$

Finally $a[b[\lambda]] = \epsilon(a\epsilon(b\lambda)) = \epsilon(ab\lambda) = (a \cdot b)[\lambda]$ and $1[\lambda] = \epsilon(\lambda) = \epsilon(\lambda 1) = \lambda$. See [11, 5.8(c), p. 108] also. Q.E.D.

1.4.2. The k-algebra map

$$\sigma\colon \mathscr{H} \to \mathrm{End}_k(K), \qquad \sigma(a)(\lambda) = a[\lambda] = \epsilon(a\lambda)$$

is called the *associated measuring representation.*

1.4.3. COROLLARY. $a\lambda = \sum_{(a)} a_{(1)}[\lambda]\, a_{(2)} = \sum_{(a)} a_{(2)}[\lambda]\, a_{(1)}$ *for* $a \in \mathscr{H}$, $\lambda \in K$.

Proof. Since $\Delta(a\lambda) = \sum_{(a)} a_{(1)} \otimes_K a_{(2)}\lambda$, $a\lambda = \sum_{(a)} \epsilon(a_{(2)}\lambda)\, a_{(1)} = \sum_{(a)} a_{(2)}[\lambda]\, a_{(1)}$. See [11, 5.8(c), p. 108] also.

1.5. Let H be a k-bialgebra. Suppose K is a left *H-module algebra* (0.7). We denote the measuring action by $a[\lambda] \in K$ for $a \in H$, $\lambda \in K$. It is easy to prove

PROPOSITION. *If* $\sum_{(a)} a_{(1)}[\lambda] \otimes a_{(2)} = \sum_{(a)} a_{(2)}[\lambda] \otimes a_{(1)}$ *in* $K \otimes H$ *for all* $a \in H$ *and* $\lambda \in K$, *then the smash product k-algebra* $K \# H$ *together with the K-coalgebra structure* $K \otimes H$ *becomes a K/k-bialgebra.*

The resulting K/k-bialgebra is denoted by $K \# H$ too. The measuring action (1.4.2) associated with this K/k-bialgebra is given by $(\lambda \# a)[\mu] = \lambda \cdot a[\mu]$. Note that the above condition is satisfied if H is *cocommutative* (cf. [11, pp. 117–118]).

1.6. Recall that F is a subalgebra of K. Suppose that K is a *finite projective* F-module. Then $\mathsf{Mod}_F(K, F)$ has a natural cocommutative F-coalgebra structure (0.9). Hence

$$\mathrm{End}_F(K) = \mathsf{Mod}_F(K, K) \simeq K \otimes_F \mathsf{Mod}_F(K, F)$$

is a cocommutative K-coalgebra and an F-algebra at the same time. Note that the left K-module structure on $\mathrm{End}_F(K)$ is given by

$$(\lambda f)(\mu) = \lambda \cdot f(\mu) \qquad \text{for} \quad f \in \mathrm{End}_F(K) \quad \text{and} \quad \lambda, \mu \in K.$$

LEMMA. *The natural action of* $\mathrm{End}_F(K)$ *on K measures K to K.*

Proof. We write $a[\lambda] = a(\lambda)$ for $a \in \mathrm{End}_F(K)$ and $\lambda \in K$. The map $a \mapsto a[\lambda]$ is left K-linear. Since

$$\mathrm{End}_F(K) = \mathsf{Mod}_K(K \otimes_F K, K)$$

is the *dual* K-coalgebra to the K-algebra $K \otimes_F K$ whose structure is given by $\lambda \mapsto \lambda \otimes 1$, it follows that the map

$$K \otimes_F K \to \mathsf{Mod}_K(\mathrm{End}_F(K), K), \qquad \lambda \otimes \mu \mapsto \{a \mapsto \lambda \cdot a[\mu]\}$$

is a K-algebra map. Hence the k-linear map

$$K \to \mathsf{Mod}_K(\mathrm{End}_F(K), K), \qquad \lambda \mapsto \{a \mapsto a[\lambda]\}$$

is a k-algebra map or equivalently the action $a[\lambda]$ measures K to K.

1.6.1. Suppose K is a *finite projective* F-module. Let $\mathscr{C}$ be a K-coalgebra and $\omega: \mathscr{C} \otimes K \to K$ a left $K \otimes F$-linear map, where K is a $K \otimes F$-module by $(\lambda \otimes \mu)(\nu) = \lambda\mu\nu$ for $\lambda, \nu \in K$ and $\mu \in F$. Let

$$\rho: \mathscr{C} \to \mathrm{End}_F(K), \qquad \xi: K \to \mathsf{Mod}_K(\mathscr{C}, K)$$

be defined by $\rho(c)(\lambda) = \omega(c \otimes \lambda) = \xi(\lambda)(c)$. The map ξ is left F-linear.

COROLLARY. *The map ω measures K to K if and only if ρ is a map of K-coalgebras if and only if ξ is a map of F-algebras.*

1.6.2. PROPOSITION. *If K is a finite projective F-module, then the K-coalgebra and the k-algebra $\mathrm{End}_F(K)$ is a cocommutative K/k-bialgebra (in fact a K/F-bialgebra).*

Proof. Exercise (the associated measuring action is the canonical one). The K/F-bialgebra structure on $\mathrm{End}_F(K)$ is the same as the one described in [11, 8.8(a), p. 122].

1.6.3. Let $\mathscr{H}$ be a K/k-bialgebra.

$$K^{\mathscr{H}} = \{\lambda \in K \mid a[\lambda] = \epsilon(a)\lambda, \forall a \in \mathscr{H}\}$$

is a subalgebra of K and a subfield of K when K is a field (cf. (0.7)). If $F \subset K^{\mathscr{H}}$, the associated measuring representation (1.4.2) gives $\sigma: \mathscr{H} \to \mathrm{End}_F(K)$. If further K is a finite projective F-module, then this is a map of K/k-bialgebras by (1.6.1).

THEOREM. [9, 1.12] *Let K be a field and $F = K^{\mathscr{H}}$. Then $[K : F] < \infty$ if and only if the image $\sigma(\mathscr{H})$ is finite dimensional as a left K-vector space. If $[K : F] < \infty$, then $\sigma(\mathscr{H}) = \mathrm{End}_F(K)$.*

Proof. View $K \otimes K$ as a K-algebra via $\lambda \mapsto \lambda \otimes 1$. Let $\mathscr{H}(K/k)$ denote the *dual* K-coalgebra to $K \otimes K$ in the sense of [7, Sect. 6.0]. Then $\mathscr{H}(K/k)$ is a left K-subspace of $\mathbf{Mod}_K(K \otimes K \;\; K) = \mathrm{End}_k(K)$. Just as Lemma 1.6, the inclusion $\mathscr{H}(K/k) \subset \mathrm{End}_k(K)$ measures K to K. It can be shown using [7, Proposition 6.0.3] that $\mathscr{H}(K/k)$ is the subset of $f \in \mathrm{End}_k(K)$ such that there are elements $g_1, \ldots, g_n$; $h_1, \ldots, h_n \in \mathrm{End}_k(K)$ such that $f(\lambda\mu) = \sum_{i=1}^{n} g_i(\lambda)\, h_i(\mu)$ for all $\lambda, \mu \in K$. It follows that $\mathscr{H}(K/k)$ is a *k-subalgebra* of $\mathrm{End}_k(K)$. The K-coalgebra and the k-algebra $\mathscr{H}(K/k)$ becomes a cocommutative K/k-bialgebra. (This is the same as the $\times_K$-bialgebra C described in [11, 6.6, p. 112], where we put $A = K$, $R = k$, and take as $\{L_\alpha\}$ all the ideals of $K \otimes K$ such that $(K \otimes K)/L_\alpha$ are finite dimensional as *left* K-vector spaces, or the unique maximal $\times_K$-coalgebra B contained in $\mathrm{End}_k(K)$ [11, 7.1, p. 114]). If $\mathscr{H}$ is a K/k-bialgebra, then the associated measuring representation $\sigma\colon \mathscr{H} \to \mathrm{End}_k(K)$ gives a map of K/k-bialgebras $\sigma\colon \mathscr{H} \to \mathscr{H}(K/k)$. (This means that $\mathscr{H}(K/k)$ is a *final* object in the category of K/k-bialgebras.)

If $K \supset F \supset k$ are fields, then $\mathscr{H}(K/F)$ is a K/k-subbialgebra of $\mathscr{H}(K/k)$.

Winter [9, 1.12] claims (without proof) that the correspondence $F \mapsto \mathscr{H}(K/F) = \mathrm{End}_F(K)$ gives a bijection from the set of intermediate fields $K \supset F \supset k$ with $[K : F] < \infty$, onto the set of K/k-subbialgebras of $\mathscr{H}(K/k)$ finite dimensional as left K-vector spaces. The theorem follows from this. Q.E.D.

1.7. We consider the category of pairs (H, ρ) where H is a *cocommutative* k-bialgebras and $\rho\colon H \to \mathrm{End}_k(K)$ a measuring representation (0.7). Let $\mathbf{\Omega}$ denote this category. We shall construct the *right adjoint* of the functor $(H, \rho) \mapsto K \# H$, $\mathbf{\Omega} \to$ (the category of cocommutative K/k-bialgebras).

1.7.1. LEMMA. *Let $\mathscr{C}$ (resp. D) be a K-coalgebra (resp. a k-coalgebra). Then $\mathscr{C} \otimes D$ is a K-coalgebra via*

$$\Delta(c \otimes d) = \sum_{(c,d)} (c_{(1)} \otimes d_{(1)}) \otimes_K (c_{(2)} \otimes d_{(2)}),$$

$$\epsilon(c \otimes d) = \epsilon(c)\, \epsilon(d)$$

for $c \in \mathscr{C}$ and $d \in D$. Let $\mathscr{H}$ be a K/k-bialgebra and $f\colon \mathscr{C} \to \mathscr{H}$, $g\colon K \otimes D \to \mathscr{H}$ be K-coalgebra maps. Then

$$\mathscr{C} \otimes D \to \mathscr{H}, \qquad c \otimes d \mapsto f(c)\, g(1 \otimes d)$$

is a K-coalgebra map.

Proof. Easy.

1.7.2. Let $C \in \mathbf{W}_k$ and $\mathscr{H}$ be a *cocommutative* K/k-bialgebra. We identify

$$\mathbf{Mod}_K(K \otimes C, \mathscr{H}) = \mathbf{Mod}_k(C, \mathscr{H})$$

the right-hand side of which is a k-algebra (0.2). If u and $v \in \mathsf{W}_K(K \otimes C, \mathscr{H})$, then

$$u * v\colon K \otimes C \to \mathscr{H},\ \lambda \otimes c \mid \to \sum_{(c)} \lambda u(1 \otimes c_{(1)})\, v(1 \otimes c_{(2)})$$

is a K-coalgebra map by (1.7.1). Hence

PROPOSITION. *The subset* $\mathsf{W}_K(K \otimes C, \mathscr{H})$ *of* $\mathsf{Mod}_k(C, \mathscr{H})$ *is a multiplicative submonoid.*

1.7.3. PROPOSITION. *Let* $\mathscr{H}$ *be a cocommutative* K/k*-bialgebra. There is a unique* k*-algebra structure on* $\prod_{K/k} \mathscr{H}$ *which makes it a* k*-bialgebra and the adjunction* (1.1.1)

$$\gamma\colon \prod_{K/k} \mathscr{H} \to \mathscr{H}$$

into a k*-algebra map. Then for each* $C \in \mathsf{W}_k$, *the monoid* $\mathsf{W}_k(C, \prod_{K/k} \mathscr{H})$ (0.1) *is canonically isomorphic with the monoid* $\mathsf{W}_K(K \otimes C, \mathscr{H})$ (1.7.2).

Proof. For each $C \in \mathsf{W}_k$, we have

$$\mathsf{W}_k\left(C, \prod_{K/k} \mathscr{H}\right) \simeq \mathsf{W}_K(K \otimes C, \mathscr{H}), \tag{1.7.3.1}$$

where the right-hand side is a monoid by (1.7.2). Since a cocommutative k-bialgebra is the same as a monoid object in W_k (0.1), there is a *unique* k-algebra structure on $\prod_{K/k} \mathscr{H}$ which makes it into a k-bialgebra and (1.7.3.1) into a monoid isomorphism for all $C \in \mathsf{W}_k$.

We claim that the adjunction

$$\gamma\colon \prod_{K/k} \mathscr{H} \to \mathscr{H}$$

is then a k-algebra map. Indeed for each $C \in \mathsf{W}_k$ and $\phi \in \mathsf{W}_k(C \otimes C, C)$ we have a commutative diagram of *monoids*:

$$\begin{array}{ccc} \mathsf{W}_k\left(C, \prod_{K/k} \mathscr{H}\right) & \simeq & \mathsf{W}_K(K \otimes C, \mathscr{H}) \\ \downarrow{\scriptstyle \mathsf{W}_k(\phi, \Pi_{K/k}\mathscr{H})} & & \downarrow{\scriptstyle \mathsf{W}_K(K \otimes \phi, \mathscr{H})} \\ \mathsf{W}_k\left(C \otimes C, \prod_{K/k} \mathscr{H}\right) & \simeq & \mathsf{W}_K(K \otimes C \otimes C, \mathscr{H}). \end{array}$$

Put $C = \prod_{K/k} \mathscr{H}$ and define $\phi_i \in \mathsf{W}_k(C \otimes C, C)$ $(i = 1, 2, 3)$ by

$$\phi_1(a \otimes b) = ab, \qquad \phi_2(a \otimes b) = a\epsilon(b) \qquad \text{and} \qquad \phi_3(a \otimes b) = \epsilon(a)b$$

for $a, b \in C = \prod_{K/k} \mathscr{H}$. Note that $\phi_2 * \phi_3 = \phi_1$ in the monoid $\mathsf{W}_k(C \otimes C, \prod_{K/k} \mathscr{H})$. Since the identity $I \in \mathsf{W}_k(C, \prod_{K/k} \mathscr{H})$ and $\gamma \in \mathsf{W}_K(K \otimes C, \mathscr{H})$ corresponds to each other, it follows that $\phi_1 \in \mathsf{W}_k(C \otimes C, \prod_{K/k} \mathscr{H})$ corresponds to

$$(\gamma \circ [K \otimes \phi_2]) * (\gamma \circ [K \otimes \phi_3]) \in \mathsf{W}_K(K \otimes C \otimes C, \mathscr{H})$$

which maps $\lambda \otimes c \otimes d \in K \otimes C \otimes C$ to $\lambda\gamma(1 \otimes c)\,\gamma(1 \otimes d)$. Since ϕ_1 corresponds to $\gamma \circ [K \otimes \phi_1]$ also, it follows that

$$\gamma(\lambda \otimes ab) = \lambda\gamma(1 \otimes a)\,\gamma(1 \otimes b), \qquad \forall a, b \in \prod_{K/k} \mathscr{H}.$$

Similarly we have $\gamma(1 \otimes 1) = 1$. Hence $\gamma: \prod_{K/k} \mathscr{H} \to \mathscr{H}$ is a k-algebra map. The uniqueness follows from:

1.7.4. LEMMA. *Let H be a cocommutative k-bialgebra and $u: H \to \prod_{K/k} \mathscr{H}$ a k-coalgebra map. Then u is a k-bialgebra map (with the k-bialgebra structure on $\prod_{K/k} \mathscr{H}$ defined in* (1.7.3)) *if and only if the composite*

$$\gamma \circ u: H \to \prod_{K/k} \mathscr{H} \to \mathscr{H}$$

is a k-algebra map.

Proof. Let ψ_1 and $\psi_2 \in \mathsf{W}_k(H \otimes H, \prod_{K/k} \mathscr{H})$ be defined by

$$\psi_1(c \otimes d) = u(cd) \qquad \text{and} \qquad \psi_2(c \otimes d) = u(c)\,u(d)$$

for $c, d \in H$. Then $\psi_1 = \psi_2$ if and only if

$$\gamma \circ [K \otimes \psi_1] = \gamma \circ [K \otimes \psi_2].$$

This is equivalent to $\gamma[u(cd)] = \gamma[u(c)]\,\gamma[u(d)]$, $\forall c, d \in H$, for $\gamma: \prod_{K/k} \mathscr{H} \to \mathscr{H}$ is a k-algebra map. Similarly $u(1) = 1$ if and only if $\gamma[u(1)] = 1$.

1.7.5. When $\mathscr{H}$ is a cocommutative K/k-bialgebra, we view $\prod_{K/k} \mathscr{H}$ as a cocommutative k-bialgebra by (1.7.3). If $\sigma: \mathscr{H} \to \mathrm{End}_k(K)$ denotes the associated measuring representation (1.4.2), then the composite

$$\rho = \sigma \circ \gamma: \prod_{K/k} \mathscr{H} \to \mathrm{End}_k(K)$$

is a measuring representation (0.7), since $\gamma: K \otimes \prod_{K/k} \mathscr{H} \to \mathscr{H}$ is a K-coalgebra map.

Thus we have made a functor

$$\mathscr{H} \mid \to \left(\prod_{K/k} \mathscr{H}, \rho \right)$$

from the category of cocommutative K/k-bialgebras to $\mathbf{\Omega}$.

It is clear that $K^{\mathscr{H}} \subset K^{\prod_{K/k}\mathscr{H}}$.

1.7.6. THEOREM. *The functor* $\mathscr{H} \mapsto (\prod_{K/k}\mathscr{H}, \rho)$ *is the right adjoint of the functor* $(H, \rho) \mapsto K \# H$, $\mathbf{\Omega} \to$ (*the category of cocommutative* K/k*-bialgebras*).

Proof. First we claim that the adjunction

$$\gamma\colon K \# \prod_{K/k} \mathscr{H} \to \mathscr{H}$$

is a map of K/k-bialgebras. We know that γ is a K-coalgebra map (and hence a *left* K-linear map) and the restriction $\gamma \mid \prod_{K/k}\mathscr{H}$ is a k-algebra map. Since the measuring representation ρ of $\prod_{K/k}\mathscr{H}$ is given by $\rho(a)(\lambda) = \gamma(1 \# a)[\lambda]$ for $a \in \prod_{K/k}\mathscr{H}$, $\lambda \in K$, it follows from (1.4.3) that $\gamma((1 \# a)(\lambda \# 1)) = \sum_{(a)} \rho(a_{(1)})(\lambda)\, \gamma(1 \# a_{(2)}) = \sum_{(a)} \gamma(a_{(1)})[\lambda]\, \gamma(1 \# a_{(2)}) = \gamma(1 \# a)\lambda$. Hence γ is a K/k-bialgebra map.

Let $(H, \rho) \in \mathbf{\Omega}$ and $u\colon H \to \prod_{K/k}\mathscr{H}$ be a *k-coalgebra map*. Let $U\colon K \# H \to \mathscr{H}$ denote the corresponding K-coalgebra map. We have only to prove that U is a map of K/k-bialgebras if and only if u is a k-bialgebra map commuting with the measuring action on K. The "if" part follows from the above claim, since

$$U = \gamma \circ [K \# u]\colon K \# H \to K \# \prod_{K/k} \mathscr{H} \to \mathscr{H}.$$

Suppose U is a K/k-bialgebra map. Then u is a k-bialgebra map by (1.7.4). If $a \in H$ and $\lambda \in K$, then

$$\begin{aligned}\rho(a)(\lambda) &= \epsilon((1 \# a)(\lambda \# 1)) = \epsilon(U(1 \# a)\,\lambda) = \gamma(1 \# u(a))[\lambda] \\ &= \rho(u(a))(\lambda)\end{aligned}$$

by (1.4.1), (1.5), and (1.7.5). Hence u commutes with the measuring action. Q.E.D.

1.8. Suppose K is a finite projective F-module. Then $\mathrm{End}_F(K)$ is a cocommutative K/k-bialgebra (1.6.2). On the other hand $(M_k(K/F), \Theta)$ (0.7) is an object in $\mathbf{\Omega}$.

PROPOSITION. $\prod_{K/k} \mathrm{End}_F(K) \simeq (M_k(K/F), \Theta)$ *in* $\mathbf{\Omega}$.

Proof. By (0.7) and (1.6.1) for each $C \in \mathbf{W}_k$

$$\mathbf{W}_K(K \otimes C, \mathrm{End}_F(K)) \simeq \mathbf{W}_k(C, M_k(K/F))$$

where the left (resp. right) hand side is a monoid by (1.7.2) (resp. since

$M_k(K/F)$ is a cocommutative k-bialgebra). Since $\Theta: M_k(K/F) \to \mathrm{End}_F(K)$ is a k-algebra map, the induced map

$$\mathsf{W}_k(C, M_k(K/F)) \hookrightarrow \mathsf{Mod}_k(C, \mathrm{End}_F(K))$$

is a monoid map. This shows that the above isomorphism is a monoid isomorphism. Hence $\prod_{K/k} \mathrm{End}_F(K) \simeq M_k(K/F)$ as k-bialgebras. Further, since the K-linear map $\bar{\Theta}: K \otimes M_k(K/F) \to \mathrm{End}_F(K)$ induced from Θ is the W_K-map corresponding to the identity $I: M_k(K/F) \to M_k(K/F)$, it follows that $\prod_{K/k} \mathrm{End}_F(K) \simeq (M_k(K/F), \Theta)$ in $\mathbf{\Omega}$. Q.E.D.

1.8.1. COROLLARY. *Let $\mathscr{H}$ be a cocommutative K/k-bialgebra. Suppose K is a finite projective F-module and $F \subset K^{\mathscr{H}}$. Then the associated map of K/k-bialgebras* (1.6.3)

$$\sigma: \mathscr{H} \to \mathrm{End}_F(K)$$

induces an $\mathbf{\Omega}$-map

$$\prod_{K/k} \sigma: \prod_{K/k} \mathscr{H} \to \prod_{K/k} \mathrm{End}_F(K) \simeq M_k(K/F)$$

which is the unique k-bialgebra map (0.7) *such that*

$$\Theta \circ \prod_{K/k} \sigma = \rho: \prod_{K/k} \mathscr{H} \to \mathrm{End}_F(K)$$

is the canonical measuring representation.

1.8.2. Note that $P(M_k(K/F)) \simeq \mathrm{Der}_k(K/F)$ (0.7) is naturally a *left K-module*. This is the same as the K-module structure on $P(\prod_{K/k} \mathrm{End}_F(K))$ (1.3) when K is a finite projective F-module.

1.9. We shall refer to (1.7) in the following form:

Let H be a cocommutative k-bialgebra and

$$\alpha: H \to M_k(K/F)$$

a homomorphism of k-bialgebras. Then $K \# H$ is a cocommutative K/k-bialgebra (1.5) such that $F \subset K^{(K\#H)}$. Hence $\prod_{K/k} (K \# H)$ is a cocommutative k-bialgebra having the canonical measuring representation $\rho: \prod_{K/k} (K \# H) \to \mathrm{End}_F(K)$ which can be identified with a k-bialgebra map (0.7)

$$\delta: \prod_{K/k} (K \# H) \to M_k(K/F),$$

which is said to be *associated* with α. The adjunction (1.1.1)

$$\iota: H \to \prod_{K/k} (K \# H)$$

is a k-bialgebra map and $\delta \circ \iota = \alpha$ by (1.7.6).

If K is a finite projective F-module, then the k-bialgebra map α can be identified with a map of K/k-bialgebras

$$\tilde{\alpha}: K \# H \to \mathrm{End}_F(K)$$

by (1.8) and we have

$$\delta = \prod_{K/k} \tilde{\alpha}: \prod_{K/k} (K \# H) \to \prod_{K/k} \mathrm{End}_F(K) = M_k(K/F).$$

1.9.1. In case of *hyperalgebras* (0.3), the above convention takes the following form:

Let H be a k-hyperalgebra and $\alpha: H \to hy_k(K/F)$ (0.7) a map of k-hyperalgebras. Let

$$H^{\#} = \left(\prod_{K/k} (K \# H)\right)^1$$

denote the irreducible component (0.3) containing 1, which is a k-hyperalgebra. Then the associated bialgebra map δ and the adjunction ι induce hyperalgebra maps

$$\delta: H^{\#} \to hy_k(K/F) \qquad \text{and} \qquad \iota: H \to H^{\#}$$

such that $\delta \circ \iota = \alpha$.

If K is a finite projective F-module, then the K/k-bialgebra map $\tilde{\alpha}$ induces

$$\delta = \left[\prod_{K/k} \tilde{\alpha}\right]^1: H^{\#} = \left[\prod_{K/k} (K \# H)\right]^1 \to \left[\prod_{K/k} \mathrm{End}_F(K)\right]^1 = hy_k(K/F).$$

1.9.2. With the same notations as above we have

$$P(H^{\#}) = K \otimes P(H)$$

by (1.3). The hyperalgebra map $\alpha: H \to hy_k(K/F)$ induces a (restricted) Lie algebra map

$$\alpha: P(H) \to P(hy_k(K/F)) = \mathrm{Der}_k(K/F).$$

The Lie algebra map induced from $\delta: H^{\#} \to hy_k(K/F)$

$$\delta: K \otimes P(H) = P(H^{\#}) \to P(hy_k(K/F)) = \mathrm{Der}_k(K/F)$$

maps $\lambda \otimes a \in K \otimes P(H)$ to $\lambda \cdot \alpha(a)$. In particular δ is left K-linear.

1.10. Suppose ℓ/k is an *algebraic* extension of fields. If $\mathscr{H}$ is a K/k-bialgebra, then $\ell \otimes \mathscr{H}$ is naturally a $\tilde{K}/\ell$-bialgebra with $\tilde{K} = \ell \otimes K$.

Let H be a cocommutative k-bialgebra with a measuring representation $\rho: H \to \mathrm{End}_k(K)$. Then $\ell \otimes H$ is a cocommutative ℓ-bialgebra and

$$\ell \otimes \rho: \ell \otimes H \to \ell \otimes \mathrm{End}_k(K) \subset \mathrm{End}_\ell(\tilde{K})$$

is a measuring representation. We have

$$\ell \otimes [K \# H] \simeq \tilde{K} \#_\ell (\ell \otimes H)$$

as $\tilde{K}/\ell$-bialgebras.

If $\mathscr{H}$ is cocommutative, then

$$\prod_{\tilde{K}/\ell} (\ell \otimes \mathscr{H}) \simeq \ell \otimes \prod_{K/k} \mathscr{H}$$

as ℓ-bialgebras with the same measuring action on $\tilde{K}$ by (1.2), (1.2.1), (1.7.4), and (1.7.5).

If $U: K \# H \to \mathscr{H}$ is the K/k-bialgebra map corresponding to an Ω-map $u: H \to \prod_{K/k} \mathscr{H}$ (1.7.6), then the $\tilde{K}/\ell$-bialgebra map $\ell \otimes U: \tilde{K} \#_\ell (\ell \otimes H) \to \ell \otimes \mathscr{H}$ corresponds to

$$\ell \otimes u: \ell \otimes H \to \ell \otimes \prod_{K/k} \mathscr{H} = \prod_{\tilde{K}/\ell} (\ell \otimes \mathscr{H}).$$

Recall that $\tilde{F} = \ell \otimes F$. The composite (0.7)

$$\ell \otimes M_k(K/F) \xrightarrow{\ell \otimes \Theta} \ell \otimes \mathrm{End}_F(K) \subset \mathrm{End}_{\tilde{F}}(\tilde{K})$$

which is a measuring representation, induces a map of ℓ-bialgebras

$$\ell \otimes M_k(K/F) \to M_\ell(\tilde{K}/\tilde{F}).$$

If K is a finite projective F-module, then this is an isomorphism. Indeed

$$\ell \otimes \mathrm{End}_F(K) \simeq \mathrm{End}_{\tilde{F}}(\tilde{K})$$

as $\tilde{K}/\ell$-bialgebras. Hence by (1.8)

$$\ell \otimes M_k(K/F) = \ell \otimes \prod_{K/k} \mathrm{End}_F(K) \simeq \prod_{\tilde{K}/\ell} \mathrm{End}_{\tilde{F}}(\tilde{K}) = M_\ell(\tilde{K}/\tilde{F})$$

as ℓ-bialgebras with the same measuring action on $\tilde{K}$.

If $\alpha: H \to M_k(K/F)$ is a k-bialgebra map and $\delta: \prod_{K/k} (K \# H) \to M_k(K/F)$ is associated with α (1.9), then the composite ℓ-bialgebra map

$$\prod_{\tilde{K}/\ell} [\tilde{K} \#_\ell (\ell \otimes H)] = \ell \otimes \prod_{K/k} (K \# H) \xrightarrow{\ell \otimes \delta} \ell \otimes M_k(K/F) \xrightarrow{\text{cano}} M_\ell(\tilde{K}/\tilde{F})$$

is associated with the composite ℓ-bialgebra map

$$\ell \otimes H \xrightarrow{\ell \otimes \alpha} \ell \otimes M_k(K/F) \xrightarrow{\text{cano}} M_\ell(\tilde{K}/\tilde{F}).$$

If K is finite projective F-module, then the ℓ-bialgebra map (1.9)

$$\widetilde{\ell \otimes \alpha}\colon \tilde{K} \#_\ell (\ell \otimes H) \to \mathrm{End}_{\tilde{F}}(\tilde{K})$$

identified with $\ell \otimes \delta$, is the same as

$$\ell \otimes \tilde{\alpha}\colon \ell \otimes [K \# H] \to \ell \otimes \mathrm{End}_F(K).$$

1.10.1. The canonical map $\ell \otimes M_k(K/F) \to M_\ell(\tilde{K}/\tilde{F})$ induces an ℓ-hyperalgebra map

$$\ell \otimes hy_k(K/F) \to hy_\ell(\tilde{K}/\tilde{F})$$

which is *injective*, since so is the restriction (0.5), (0.7)

$$\ell \otimes P(hy_k(K/F)) = \ell \otimes \mathrm{Der}_k(K/F) \subset \mathrm{Der}_\ell(\tilde{K}/\tilde{F}) = P(hy_\ell(\tilde{K}/\tilde{F})).$$

If K is a finite projective F-module, then

$$\ell \otimes hy_k(K/F) \xrightarrow{\simeq} hy_\ell(\tilde{K}/\tilde{F})$$

since $\ell \otimes hy_k(K/F) = [\ell \otimes M_k(K/F)]^1$ (0.3).

Let H be a k-hyperalgebra and

$$\alpha\colon H \to hy_k(K/F)$$

a hyperalgebra map. We have (0.3)

$$\ell \otimes H^* = \ell \otimes \left[\prod_{K/k} (K \# H)\right]^1 = \left[\ell \otimes \prod_{K/k} (K \# H)\right]^1$$

$$= \left[\prod_{\tilde{K}/\ell} \{\tilde{K} \#_\ell (\ell \otimes H)\}\right]^1 = (\ell \otimes H)^*.$$

The composite

$$\ell \otimes \delta\colon \ell \otimes H^* \to \ell \otimes hy_k(K/F) \xrightarrow{\subset\ \mathrm{cano}} hy_\ell(\tilde{K}/\tilde{F})$$

is associated with the composite ℓ-hyperalgebra map

$$\ell \otimes \alpha\colon \ell \otimes H \to \ell \otimes hy_k(K/F) \xrightarrow{\subset\ \mathrm{cano}} hy_\ell(\tilde{K}/\tilde{F}).$$

2. Pseudohyperalgebras

Suppose k is of characteristic $p > 0$.

2.1. Let C be a connected cocommutative k-coalgebra. Let

$$\gamma^i\colon C \to k^{-i} \otimes C$$

be the iterated Ψ-map (0.8). Put

$$U_i = P(\Psi^i(C))$$

which is a k^{-i}-subspace of $k^{-i} \otimes P(C)$, since $\Psi^i(C)$ is a k^{-i}-subcoalgebra of $k^{-i} \otimes C$ (0.8). The sequence

$$\xi(C) = (U_0, U_1, U_2, ..., U_n, ...)$$

satisfies:

2.1.1. U_0 is a vector space over k,

2.1.2. U_i is a k^{-i}-subspace of $k^{-i} \otimes U_0$, $\forall i \geqslant 0$,

2.1.3. $U_{i+1} \subset k^{-i-1} \otimes_{k^{-i}} U_i$, $\forall i \geqslant 0$.

2.2. If ℓ/k is an extension of fields, then $\Psi^i: \ell \otimes C \to \ell^{-i} \otimes_\ell (\ell \otimes C)$ is obtained from $\Psi^i: C \to k^{-i} \otimes C$ by scalar extension (0.8). Hence

LEMMA. *For each connected cocommutative k-coalgebra C, the invariant*

$$\xi_\ell(\ell \otimes C) = (\tilde{U}_0, \tilde{U}_1, ..., \tilde{U}_n, ...)$$

of the ℓ-coalgebra $\ell \otimes C$ is given by

$$\tilde{U}_i = \ell^{-i} \otimes_{k^{-i}} U_i .$$

2.3. If D is a subcoalgebra of a connected cocommutative k-coalgebra C, then $\xi(D) \subset \xi(C)$ in the sense that $\xi(D) = (U_0', U_1', U_2', ...)$ with $U_i' \subset U_i$.

When k is *perfect*, the invariant $\xi(C)$ is a descending chain

$$U_0 \supset U_1 \supset U_2 \supset \cdots$$

of k-subspaces of $U_0 = P(C)$.

2.4. A connected cocommutative k-coalgebra C is a *pseudohyperalgebra* (called a *pseudo-subbialgebra* of $B(U)$ in [4, II]) if there is a k-hyperalgebra whose underlying coalgebra is isomorphic to C.

THEOREM. *Let C be a k-pseudohyperalgebra and D a pseudohyperalgebra and a subcoalgebra of C. If $\xi(D) = \xi(C)$, then $D = C$.*

Proof. Let ℓ be the *perfect closure* of k. Then $\xi_\ell(\ell \otimes D) = \xi_\ell(\ell \otimes C)$ by (2.2) and $\ell \otimes D \subset \ell \otimes C$ are ℓ-pseudohyperalgebras. Hence we can reduce to the case k is perfect.

2.4.1. For each k-coalgebra C, let $\{C_n\}$ denote the coradical filtration (0.5) and put

$$\mathrm{gr}(C) = \bigoplus_{n=0}^{\infty} C_n/C_{n-1}, \qquad \text{where} \quad C_{-1} = 0.$$

This is a *graded coalgebra* [7, Sect. 11.1].

If H is an irreducible k-bialgebra (i.e., $H_0 = k$) then $\mathrm{gr}(H)$ is a *commutative* graded bialgebra [7, Theorem 11.2.5]. If L is another irreducible k-bialgebra and $\phi: L \to H$ a *coalgebra map*, then the associated map of graded coalgebras $\mathrm{gr}(\phi)$: $\mathrm{gr}(L) \to \mathrm{gr}(H)$ becomes automatically a map of graded bialgebras [7, Theorem 11.2.5].

This means in particular that if C is a pseudohyperalgebra, then all hyperalgebra structures on C induce the *same* bialgebra structure on $\mathrm{gr}(C)$. Hence if $\phi: D \to C$ is a coalgebra map where D and C are pseudohyperalgebras, then $\mathrm{gr}(\phi)$: $\mathrm{gr}(D) \to \mathrm{gr}(C)$ is a graded bialgebra map. Note that if $\phi: D \hookrightarrow C$, then $\mathrm{gr}(\phi)$: $\mathrm{gr}(D) \hookrightarrow \mathrm{gr}(C)$.

2.4.2. For each k-vector space U, we defined in (0.6) a k-hyperalgebra $B_k(U)$. Let X be a basis for U and $\mathbb{N}^{(X)}$ the set of functions $f: X \to \mathbb{N}$ (the set of integers $\geqslant 0$) with finite support.

For $f \in \mathbb{N}^{(X)}$ let $|f| = \sum_{x \in X} f(x)$. For $f, g \in \mathbb{N}^{(X)}$ let $f + g \in \mathbb{N}^{(X)}$ be defined by $(f+g)(x) = f(x) + g(x)$ for $x \in X$. Let

$$\binom{f}{g} = \prod_{x \in X} \binom{f(x)}{g(x)} \qquad \text{where} \quad \binom{a}{b} = 0 \quad \text{if} \quad b > a.$$

It is shown [4, II, 4.2] that $B_k(U)$ has a basis $\{u_{(f)} \mid f \in \mathbb{N}^{(X)}\}$ where

$$\Delta[u_{(f)}] = \sum_{g+h=f} u_{(g)} \otimes u_{(h)},$$

$$\epsilon(u_{(f)}) = \delta_{f,0},$$

$$u_{(f)} u_{(g)} = \binom{f+g}{f} u_{(f+g)},$$

$$1 = u_{(0)}.$$

The graduation

$$B(U)(n) = \sum_{|f|=n} k u_{(f)}, \qquad n = 0, 1, 2, \ldots$$

does not depend on the basis X and gives $B(U) \simeq \mathrm{gr}(B(U))$ as graded bialgebras.

We can identify $U = P(B(U)) = B(U)(1)$.

2.4.3. Suppose k is perfect. Let C be a pseudohyperalgebra and a subcoalgebra of $B_k(U)$ containing U. Put

$$\xi(C) = (U = U_0 \supset U_1 \supset U_2 \supset \cdots).$$

Fix a sufficiently large integer N. Let X be a basis for U such that there is a sequence $X = X_0 \supset X_1 \supset X_2 \supset \cdots \supset X_N$ such that X_i is a basis for U_i, $i = 0, 1, \ldots, N$. For $x \in X$, let $(x) \leqslant N$ be the largest integer with $x \in X_{(x)}$.

By (2.4.2) $\mathrm{gr}(C)$ is a graded subcoalgebra of $\mathrm{gr}(B_k(U)) = B_k(U)$.

LEMMA. *For each $m < p^{N+1}$, the set*

$$\{u_{(f)} \mid |f| = m \quad \text{and} \quad f(x) < p^{(x)+1}, \forall x \in X\}$$

forms a basis for $\mathrm{gr}(C)(m) = C_m/C_{m-1}$.

Proof. Let $P(m)$ denote the subspace spanned by the above set. The inclusion $\mathrm{gr}(C)(m) \subset P(m)$, $\forall m < p^{N+1}$, follows from [5, Lemma 6].

We prove the opposite inclusion $P(m) \subset \mathrm{gr}(C)(m)$ by induction. This is clear if $m = 0$ or 1. Suppose $u_{(f)} \in P(m)$.

Case $f = f' + f''$ for some $f' \neq 0, f'' \neq 0$ with $\mathrm{Supp}(f') \cap \mathrm{Supp}(f'') = \varnothing$. Since $u_{(f')}$ and $u_{(f'')} \in \mathrm{gr}(C)$ by the induction hypothesis and that $\mathrm{gr}(C) \subset B(U)$ is a graded subbialgebra, it follows that

$$u_{(f)} = u_{(f')}u_{(f'')} \in \mathrm{gr}(C)(m).$$

Hence we can reduce to the case $f = m\delta_x$, with $x \in X$, where $\delta_x\colon X \to \mathbb{N}$, $y \mapsto \delta_{xy}$.

Case m is not a power of p. There are integers $i > 0$ and $j > 0$ with $m = i + j$ and $\binom{m}{i} \not\equiv 0 \bmod p$. Then $i\delta_x$ and $j\delta_x \in \mathrm{gr}(C)$ by the induction hypothesis. Hence as above

$$u_{(i\delta_x)}u_{(j\delta_x)} = \binom{m}{i} u_{(f)} \in \mathrm{gr}(C).$$

Since $\binom{m}{i} \neq 0$ in k, $u_{(f)} \in \mathrm{gr}(C)(m)$.

Case $m = p^e$. It follows from (0.8.2) that the coradical filtration on $\mathscr{V}^r(C)$ is given by

$$\mathscr{V}^r(C)_n = \mathscr{V}^r(C) \cap C_n = \mathscr{V}^r(C_{p^r n}).$$

Since $p^e = f(x) < p^{(x)+1}$, $e \leqslant (x)$. Hence $x \in \mathscr{V}^e(C) \cap C_1 = \mathscr{V}^e(C_{p^e})$. There is an element

$$c = \sum_i \lambda_i u_{(f_i)} + d \in C_{p^e}$$

with $\mathscr{V}^e(c) = x$, where $\lambda_i \neq 0 \in k$, $f_i \in \mathbb{N}^{(X)}$ with $|f_i| = p^e$ and $d \in C_{p^e-1}$. Since $\mathrm{gr}(C)(p^e) \subset P(p^e)$, we have $u_{(f_i)} \in P(p^e)$ for all i. Applying the iterated $\mathscr{V}$-map $\mathscr{V}^e$, we see that

$$\lambda_i = 1 \quad \text{if } f_i = p^e\delta_x\,; \qquad \mathrm{Supp}(f_i) \neq \{\text{one point}\} \quad \text{if } f_i \neq p^e\delta_x\,.$$

We know that $u_{(f_i)} \in \mathrm{gr}(C)(p^e)$ if $\mathrm{Supp}(f_i) \neq \{\text{one point}\}$. Hence $u_{(f)} \in \mathrm{gr}(C)(p^e)$. Q.E.D.

2.4.4. We can prove Theorem 2.4. We can assume k is perfect. Put

$$\xi(D) = \xi(C) = (U_0 \supset U_1 \supset U_2 \supset \cdots).$$

Embed C into $B_k(U_0)$ as a subcoalgebra so that $\pi \mid U_0$ is the identity. Thus $U_0 \subset D \subset C \subset B_k(U_0)$. It follows directly from (2.4.3) that

$$\mathrm{gr}(D)(m) = \mathrm{gr}(C)(m) \subset B_k(U_0)(m)$$

for all $m < p^{N+1}$. Since N can be arbitrarily chosen, we have $\mathrm{gr}(D) = \mathrm{gr}(C)$. This means $D = C$. Q.E.D.

2.5. The invariant $\xi(C)$ *classifies* the graded bialgebras $\mathrm{gr}(C)$. More precisely we can prove:

Let U be a k-vector space and

$$\xi = (U_0\,,\ U_1\,,\ U_2\,,\ldots)$$

a sequence satisfying (2.1.1, 2, 3) *and $U_0 = U$. There is a unique graded subbialgebra $A(\xi)$ of $B_k(U)$ such that $\xi(A(\xi)) = \xi$.*

Let C be a pseudohyperalgebra and a subcoalgebra of $B_k(U)$ containing U. If $\xi = \xi(C)$, then $\mathrm{gr}(C) = A(\xi)$. In particular we have

$$\xi(C) = \xi(\mathrm{gr}(C)).$$

If C and D are two pseudohyperalgebras, then $\mathrm{gr}(C) \simeq \mathrm{gr}(D)$ as coalgebras or graded coalgebras or graded bialgebras if and only if $\xi(C) \simeq \xi(D)$.

The proof will be published elsewhere. This is not used in this paper.

2.6. Suppose k is *perfect*, let C be a k-pseudohyperalgebra and put $\xi(C) = (U_0 \supset U_1 \supset U_2 \supset \cdots)$. Theorem 0.8.1 implies that U_i is the set of elements in $P(C) = U_0$ over which there is a $(p^{i+1} - 1)$-SDP in C.

2.7. Let K be a commutative k-algebra and H a subhyperalgebra of $hy_k(K)$. The inclusion $H \hookrightarrow hy_k(K)$ induces a k-hyperalgebra map (1.9.1)

$$\delta\colon H^{\#} \to hy_k(K).$$

Suppose that $\delta(H^{\#}) \subset H$.

If ℓ/k is an algebraic extension of fields, then $\ell \otimes H \subset \ell \otimes hy_k(K) \subset hy_\ell(\tilde{K})$ with $\tilde{K} = \ell \otimes K$ and we have $\delta[(\ell \otimes H)^{\#}] \subset \ell \otimes H$ (1.10.1).

Let $\xi(H) = (U_0, U_1, U_2, \ldots)$. $P(H) = U_0$ is a k-subspace of $P(hy_k(K)) = \mathrm{Der}_k(K)$ which is a left K-module.

LEMMA. *If $\delta(H^{\#}) \subset H$, then U_i is a $k^{-i} \otimes K$-submodule of $k^{-i} \otimes \mathrm{Der}_k(K)$ for all $i \geqslant 0$.*

Proof. Let $\ell =$ the perfect closure of k. Put $\xi_\ell(\ell \otimes H) = (\tilde{U}_0 \supset \tilde{U}_1 \supset \tilde{U}_2 \supset \cdots)$. Then $\tilde{U}_i = \ell \otimes_{k^{-i}} U_i \subset \ell \otimes_{k^{-i}} (k^{-i} \otimes \mathrm{Der}_k(K)) = \ell \otimes \mathrm{Der}_k(K) \subset \mathrm{Der}_\ell(\tilde{K})$. Since

$$\tilde{K} = \ell \otimes K = \ell \otimes_{k^{-i}} (k^{-i} \otimes K),$$

it is enough to show that each $\tilde{U}_i$ is a $\tilde{K}$-submodule of $\mathrm{Der}_\ell(\tilde{K})$. Since $\delta[(\ell \otimes H)^{\#}] \subset \ell \otimes H$, we can reduce to the case k is perfect.

Suppose k is perfect. Then $U_0 \supset U_1 \supset U_2 \supset \cdots$. If $x \in U_i$, there is a $(p^{i+1} - 1)$-SDP $\{x_n\}_{0 \leqslant n < p^{i+1}}$ in H over x (2.6). Then $\{\iota(x_n)\}_{0 \leqslant n < p^{i+1}}$ is a $(p^{i+1} - 1)$-SDP in $H^{\#}$ where $\iota: H \to H^{\#}$ is the adjunction. We can view this sequence as a $(p^{i+1} - 1)$-SDP in the K-coalgebra $K \otimes H$ by (1.3). Hence for each $\lambda \in K$

$$\{\lambda^n \cdot \iota(x_n)\}_{0 \leqslant n < p^{i+1}}$$

is a $(p^{i+1} - 1)$-SDP in $K \otimes H$. We view this sequence as a $(p^{i+1} - 1)$-SDP in $H^{\#}$ again. Then the SDP $\{\delta(\lambda^n \cdot \iota(x_n))\}_{0 \leqslant n < p^{i+1}}$ clearly lies over λx $(\in \mathrm{Der}_k(K))$. Since $\delta(H^{\#}) \subset H$, this means that $x \in U_i$. Hence U_i is a K-submodule of $\mathrm{Der}_k(K)$. Q.E.D.

2.8. With the same notations as above, suppose k is *perfect*. Let

$$\mathfrak{a}_i = \{\lambda \in K \mid \lambda^{p^i} = 0\}.$$

Thus $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \cdots$ are nil ideals of K. Let U_∞ be the set of elements in $P(H)$ over which there is an ∞-SDP in H. Hence $U_\infty \subset \bigcap_n U_n$, where $\xi(H) = (U_0 \supset U_1 \supset U_2 \supset \cdots)$.

LEMMA. $\mathfrak{a}_i U_{i-1} \subset U_\infty$ *for all* $i > 0$.

Proof. Let $x \in U_{i-1}$. There is a $(p^i - 1)$-SDP $\phi: B_{k,p^{i-1}} \to H$ lying over x. Let $\lambda \in \mathfrak{a}_i$. Define a K-linear map

$$f: K \otimes B_k \to K \otimes B_{k,p^{i-1}}$$

by $f(1 \otimes b_j) = \lambda^j \otimes b_j$ if $j < p^i$ and $=0$ if $j \geqslant p^i$. This is a K-coalgebra map since $\lambda^{p^i} = 0$. The composite K-coalgebra map

$$K \otimes B_k \xrightarrow{f} K \otimes B_{k,p^i-1} \xrightarrow{K\otimes\phi} K \otimes H$$

corresponds to a k-coalgebra map

$$\psi\colon B_k \to \left[\prod_{K/k} (K \otimes H)\right]^1 = H^*$$

which is an ∞-SDP in H^*. If we identify (1.9.2)

$$P(H^*) = P(K \otimes H) = K \otimes P(H)$$

we have $\psi(b_1) = \lambda \otimes x$. Hence the composite

$$B_k \xrightarrow{\psi} H^* \xrightarrow{\delta} H$$

is an ∞-SDP in H lying over λx. Therefore $\lambda x \in U_\infty$. Q.E.D.

3. The Galois Subhyperalgebras $hy_k(K/F)$

Let K/k be an extension of fields of characteristic $p > 0$. Let H be a subhyperalgebra of $hy_k(K)$. Put $F = K^H$ which is a subfield of K (0.7). The inclusion $H \hookrightarrow hy_k(K/F)$ induces a k-hyperalgebra map $\delta\colon H^* \to hy_k(K/F)$ (1.9.1). The purpose of this section is to prove:

3.1. Theorem. *Suppose* $[K:F] < \infty$. *Then* $H = hy_k(K/F)$ *if and only if* $\delta(H^*) \subset H$.

The "only if" part is obvious (see (1.7.5)). The "if" part is proved step by step. We fix the following notations:

H is a subhyperalgebra of $hy_k(K/F)$ with $F = K^H$, $\delta(H^*) \subset H$ and $[K:F] < \infty$.

$\xi(H) = (U_0, U_1, U_2, \ldots)$. Then $P(H) = U_0$ is a K-subspace of $\mathrm{Der}_k(K/F)$ and U_i is a $k^{-i} \otimes K$-submodule of $k^{-i} \otimes U_0$ (2.7).

ℓ is the perfect closure of k.

$\tilde{K} = \ell \otimes K, \tilde{F} = \ell \otimes F$. We identify $\ell \otimes hy_k(K/F) = hy_\ell(\tilde{K}/\tilde{F})$ (1.10.1).

$\xi_\ell(\ell \otimes H) = (\tilde{U}_0 \supset \tilde{U}_1 \supset \tilde{U}_2 \supset \cdots)$, where $\tilde{U}_i = \ell \otimes_{k^{-i}} U_i$ (2.2).

$\tilde{U}_\infty = \{x \in P(\ell \otimes H) \mid$ There is an ∞-SDP in $\ell \otimes H$ lying over $x\}$. Thus $\tilde{U}_\infty \subset \bigcap_i \tilde{U}_i$.

$\mathfrak{a}_i = \{\lambda \in \tilde{K} \mid \lambda^{p^i} = 0\}$. Hence $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \cdots$ and $\mathfrak{a}_i \tilde{U}_{i-1} \subset \tilde{U}_\infty$ (2.8).

3.2. An arrow $u: a \to b$ in an *abelian* category A is *quasi-split* if u factors as $u: a \xrightarrow{v} c \xrightarrow{w} b$ where v is an epimorphism and there is an arrow $r: b \to c$ with $r \circ w = 1$.

If $u: M \to N$ is a quasi-split arrow in Mod_R where R is a commutative ring, then for any commutative overring S/R, $S \otimes_R u: S \otimes_R M \to S \otimes_R N$ is quasi-split in Mod_S.

LEMMA. *The $\tilde{K}/\mathfrak{a}_i$-linear map*

$$\tilde{U}_i/\mathfrak{a}_i\tilde{U}_i \to \tilde{U}_0/\mathfrak{a}_i\tilde{U}_0$$

induced from the inclusion $\tilde{U}_i \hookrightarrow \tilde{U}_0$ is quasi-split for all $i \geqslant 0$.

Proof. Fix i and put $S = \tilde{K}/\mathfrak{a}_i$ and $R = (k^{-i} \otimes K)/\mathfrak{a}_i'$ with $\mathfrak{a}_i' = \mathfrak{a}_i \cap (k^{-i} \otimes K)$. The above S-linear map is of the form $S \otimes_R u$ where

$$u: U_i/\mathfrak{a}_i'U_i \to (k^{-i} \otimes U_0)/\mathfrak{a}_i'\,(k^{-i} \otimes U_0)$$

is the R-linear map induced from the inclusion $U_i \hookrightarrow k^{-i} \otimes U_0$. We have only to prove that u is quasi-split. The composite ring homomorphism

$$k^{-i} \otimes K \hookrightarrow \tilde{K} \xrightarrow{f^i} \tilde{K}$$

where $f^i(\lambda) = \lambda^{p^i}$, induces $R \hookrightarrow \tilde{K}$. Since $f^i(k^{-i} \otimes K) = kK^{p^i}$ is a field, R is a field. Hence u is quasi-split. Q.E.D.

3.3. The above lemma implies that the submodule $\tilde{U}_i/(\tilde{U}_i \cap \mathfrak{a}_i\tilde{U}_0)$ of $\tilde{U}_0/\mathfrak{a}_i\tilde{U}_0$ is a direct summand for all $i \geqslant 0$.

3.3.1. LEMMA. [1, p. 88] *Let A be a (noncommutative) ring and J a two-sided nil ideal of A. Then each idempotent in A/J can be lifted to an idempotent in A.*

3.3.2. LEMMA. *Let R be a commutative ring and $\mathfrak{a}$ a nil-ideal of R. Then for each $n > 0$, $M_n(\mathfrak{a})$ is a nil-ideal of $M_n(R)$, the $n \times n$ matrix ring over R.*

Proof. We can reduce to the case $\mathfrak{a}$ is finitely generated. Since then $\mathfrak{a}$ is nilpotent, the result is clear.

3.3.3. COROLLARY. *With the same notations as above, let M be an n-dimensional free left R-module. If $\overline{N}$ is a direct summand $R/\mathfrak{a}$-submodule of $M/\mathfrak{a}M$, then there are submodules P and Q of M such that $M = P \oplus Q$ and $\overline{N} = P/\mathfrak{a}P$.*

Proof. Since $\mathrm{End}_R(M) \simeq M_n(R)$ and $\mathrm{End}_{R/\mathfrak{a}}(M/\mathfrak{a}M) \simeq M_n(R/\mathfrak{a})$, each idempotent in $\mathrm{End}_{R/\mathfrak{a}}(M/\mathfrak{a}M)$ can be lifted to an idempotent in $\mathrm{End}_R(M)$.

3.3.4. Since $[K:F] < \infty$, $\mathrm{Der}_k(K/F)$ is finite dimensional over K and so is U_0. Hence $\tilde{U}_0$ is a finite free $\tilde{K}$-module.

Since $\tilde{U}_1/\mathfrak{a}_1\tilde{U}_0$ (note that $\mathfrak{a}_1\tilde{U}_0 \subset \tilde{U}_\infty \subset \tilde{U}_1$) is a direct summand $\tilde{K}/\mathfrak{a}_1$-submodule of $\tilde{U}_0/\mathfrak{a}_1\tilde{U}_0$, there is a direct sum decomposition

$$\tilde{U}_0 = P_0 \oplus Q_1$$

as $\tilde{K}$-modules such that $Q_1/\mathfrak{a}_1Q_1 = \tilde{U}_1/\mathfrak{a}_1\tilde{U}_0$ by (3.3.3). Since $\mathfrak{a}_1\tilde{U}_0 \subset \tilde{U}_1$, we have $Q_1 \subset \tilde{U}_1$ and hence

$$\tilde{U}_1 = (\tilde{U}_1 \cap P_0) \oplus Q_1 \supset \mathfrak{a}_1P_0 \oplus \mathfrak{a}_1Q_1 = \mathfrak{a}_1\tilde{U}_0.$$

Therefore $\tilde{U}_1 \cap P_0 = \mathfrak{a}_1P_0$. Thus we have proved:

LEMMA. *There are $\tilde{K}$-submodules P_0 and Q_1 of $\tilde{U}_0$ such that*

$$\tilde{U}_0 = P_0 \oplus Q_1, \qquad \tilde{U}_1 = \mathfrak{a}_1P_0 \oplus Q_1.$$

3.3.5. LEMMA. *$\tilde{K}$ is local. Hence all finitely generated projective $\tilde{K}$-modules are free* [1, p. 91].

Proof. If $x \in \tilde{K}$, then $x^{p^r} \in K$ for some $r > 0$.

3.3.6. Assume that there are $\tilde{K}$-submodules of $\tilde{U}_0$

$$P_0, P_1, P_2, \ldots, P_{n-1} \text{ and } Q_n$$

such that

$$\tilde{U}_i = \mathfrak{a}_1P_0 \oplus \mathfrak{a}_2P_1 \oplus \cdots \oplus \mathfrak{a}_iP_{i-1} \oplus P_i \oplus \cdots \oplus P_{n-1} \oplus Q_n$$

for all $i = 0, 1, \ldots, n$. This means in particular

$$\tilde{U}_0 = P_0 \oplus P_1 \oplus \cdots \oplus P_{n-1} \oplus Q_n.$$

This is valid when $n = 1$ (3.3.4).

Since $P_i \subset \tilde{U}_i$ for $i = 0, 1, \ldots, n-1$, we have by (2.8)

$$\mathfrak{a}_1P_0 \oplus \cdots \oplus \mathfrak{a}_nP_{n-1} \subset \tilde{U}_\infty \subset \tilde{U}_{n+1}.$$

Since $\tilde{U}_{n+1} \subset \tilde{U}_n = \mathfrak{a}_1P_0 \oplus \cdots \oplus \mathfrak{a}_nP_{n-1} \oplus Q_n$, it follows that

$$\tilde{U}_{n+1} = \mathfrak{a}_1P_0 \oplus \cdots \oplus \mathfrak{a}_nP_{n-1} \oplus (\tilde{U}_{n+1} \cap Q_n).$$

Let $\pi\colon \tilde{U}_0 \to \tilde{U}_0/\mathfrak{a}_{n+1}\tilde{U}_0$ be the canonical projection. Then

$$\pi(\tilde{U}_{n+1}) = \pi(\tilde{U}_{n+1} \cap Q_n) \subset \pi(Q_n)$$

since $\mathfrak{a}_1P_0 + \cdots + \mathfrak{a}_nP_{n-1} \subset \mathfrak{a}_{n+1}\tilde{U}_0$. Since $\pi(\tilde{U}_{n+1})$ is a direct summand of $\tilde{U}_0/\mathfrak{a}_{n+1}\tilde{U}_0$, it is a direct summand of $\pi(Q_n)$.

Since $Q_n \subset \tilde{U}_n$, $\mathfrak{a}_{n+1}Q_n \subset \tilde{U}_\infty \cap Q_n \subset \tilde{U}_{n+1} \cap Q_n$. Hence $\pi(\tilde{U}_{n+1}) = (\tilde{U}_{n+1} \cap Q_n)/\mathfrak{a}_{n+1}Q_n$ is a direct summand of $\pi(Q_n) = Q_n/\mathfrak{a}_{n+1}Q_n$ as a $\tilde{K}/\mathfrak{a}_{n+1}$-module. Since Q_n is a finite free $\tilde{K}$-module (3.3.5) and $\mathfrak{a}_{n+1}$ is nil, there are $\tilde{K}$-submodules P_n and Q_{n+1} of Q_n such that

$$Q_n = P_n \oplus Q_{n+1}, \qquad \tilde{U}_{n+1} \cap Q_n = \mathfrak{a}_{n+1}P_n \oplus Q_{n+1}$$

by the same reason as (3.3.4).

This completes the induction process and proves:

LEMMA. *There are $\tilde{K}$-submodules of $\tilde{U}_0$*

$$P_0, P_1, \ldots, P_n, \ldots; \qquad Q_0, Q_1, \ldots, Q_n, \ldots$$

such that

(i) $Q_n = P_n \oplus Q_{n+1}$, $\forall n \geqslant 0$,

(ii) $\tilde{U}_n = \mathfrak{a}_1P_0 \oplus \mathfrak{a}_2P_1 \oplus \cdots \oplus \mathfrak{a}_nP_{n-1} \oplus Q_n$, $\forall n \geqslant 0$.

Note that this implies in particular $\tilde{U}_0 = Q_0$.

3.3.7. With the same notations as above we have

$$\tilde{U}_0 = P_0 \oplus P_1 \oplus \cdots \oplus P_{n-1} \oplus Q_n$$

for all $n \geqslant 0$. Since $\tilde{U}_0$ is finite free over $\tilde{K}$, there is an integer $N > 0$ such that

$$P_N = P_{N+1} = P_{N+2} = \cdots = 0,$$
$$Q_N = Q_{N+1} = Q_{N+2} = \cdots = Q.$$

Note that $Q \subset \bigcap_n \tilde{U}_n$.

LEMMA. $Q = 0$.

Proof. Suppose $Q \neq 0$. Since Q is a free $\tilde{K}$-submodule of $\tilde{U}_0 \subset \mathrm{Der}_\ell(\tilde{K}/\tilde{F})$, there is an element $D \in Q$ such that

$$\{\lambda \in \tilde{K} \mid \lambda D = 0\} = 0.$$

Let $\{x_1, \ldots, x_s\}$ be an F-basis for K. Since K/F is purely inseparable [7, Theorem 10.2.1(c)] there is an integer $r > 0$ such that $x_i^{p^r} \in F$, $\forall i$. Since $D \in Q \subset \tilde{U}_r$, there is a $(p^{r+1} - 1)$-SDP $\{D_0, D_1, \ldots, D_{p^{r+1}-1}\}$ in $\ell \otimes H$ with $D = D_1$. Then

$$0 = D_{p^r}(x_i^{p^r}) = D(x_i)^{p^r}.$$

Hence $D(x_i) \in \mathfrak{a}_r$ for all i. Thus

$$J = \tilde{K}D(x_1) + \cdots + \tilde{K}D(x_s),$$

which is contained in $\mathfrak{a}_r$ is a nilpotent ideal of $\tilde{K}$. $J \neq 0$ since $D \neq 0$. If $J^M = 0$ but $J^{M-1} \neq 0$, then

$$J^{M-1} \subset \{\lambda \in \tilde{K} \mid \lambda D = 0\},$$

a contradiction. Q.E.D.

3.4. It follows that there are $\tilde{K}$-submodules of $\tilde{U}_0$

$$P_0, P_1, \ldots, P_{N-1}$$

such that

$$\begin{aligned}
\tilde{U}_0 &= P_0 \oplus P_1 \oplus \cdots \oplus P_{N-1}, \\
\tilde{U}_n &= \mathfrak{a}_1 P_0 \oplus \mathfrak{a}_2 P_1 \oplus \cdots \oplus \mathfrak{a}_n P_{n-1} \oplus P_n \oplus \cdots \oplus P_{N-1}, \\
&\qquad\qquad\qquad\qquad\qquad\qquad n = 1, 2, \ldots, N-1, \\
\tilde{U}_n &= \mathfrak{a}_1 P_0 \oplus \mathfrak{a}_2 P_1 \oplus \cdots \oplus \mathfrak{a}_N P_{N-1}, \qquad n = N, N+1, \ldots, \infty.
\end{aligned}$$

Since the $\tilde{K}$-modules P_n are free (3.3.5), there is a $\tilde{K}$-basis X for $\tilde{U}_0$ such that there is a sequence $X = X_0 \supset X_1 \supset \cdots \supset X_{N-1}$ such that $X_i - X_{i+1}$ is a $\tilde{K}$-basis for P_i, $i = 0, 1, \ldots, N-1$. (The set X is finite.)

For each $x \in X$, let (x) be the largest integer $< N$ with $x \in X_{(x)}$. Note that $\{x \in X \mid (x) = i\}$ is a $\tilde{K}$-basis for P_i.

Let Λ be the set of functions $f: X \to \mathbb{N}$ such that $f(x) < p^{(x)+1}$ for all $x \in X$.

Let C be the ℓ-coalgebra with a free basis $\{v_{(f)} \mid f \in \Lambda\}$ where

$$\Delta(v_{(f)}) = \sum_{f=g+h} v_{(g)} \otimes v_{(h)},$$

$$\epsilon(v_{(f)}) = \delta_{f,0}.$$

Then C is an ℓ-pseudohyperalgebra (2.4). Indeed the multiplication

$$v_{(f)} v_{(g)} = \binom{f+g}{f} v_{(f+g)}$$

(which is well defined since $\binom{f+g}{f} = 0$ if $f + g \notin \Lambda$) makes C into an ℓ-hyperalgebra with $1 = v_{(0)}$.

Totally order X. For each $x \in X$, let $\{x_i\}$ be a $(p^{(x)+1} - 1)$-SDP in the ℓ-hyperalgebra $\ell \otimes H$ lying over x. (Note that $x \in P_{(x)} \subset \tilde{U}_{(x)}$).

Define an ℓ-linear map

$$\phi: C \to \ell \otimes H$$

by $\phi(v_{(f)}) = \prod_{x \in X} x_{f(x)}$, $f \in \Lambda$, the right-hand side of which is defined by the total order fixed on X. Then ϕ is an ℓ-coalgebra map whose restriction

$$\phi \mid P(C): P(C) \to \ell \otimes U_0 = \tilde{U}_0$$

is an *injection* onto the ℓ-subspace of $\tilde{U}_0$ spanned by X.

Let $C^{\#}$ denote the irreducible component $[\prod_{\tilde{K}/\ell}(\tilde{K} \otimes_\ell C)]^1$ where 1 denotes the canonical group-like element. Since C has an ℓ-hyperalgebra structure and there is at least one measuring representation $\rho: C \to \mathrm{End}_\ell(\tilde{K})$ (e.g., the trivial one), it follows from (1.9.1) that $C^{\#}$ is an *ℓ-pseudohyperalgebra* with

$$P(C^{\#}) = P(\tilde{K} \otimes_\ell C) = \tilde{K} \otimes_\ell P(C) = \tilde{K}X \qquad (1.3).$$

The ℓ-coalgebra map ϕ induces an ℓ-coalgebra map

$$\prod_{\tilde{K}/\ell} [\tilde{K} \otimes_\ell \phi]: C^{\#} \to (\ell \otimes H)^{\#} = \ell \otimes H^{\#}.$$

Put

$$\psi: C^{\#} \xrightarrow{\Pi_{\tilde{K}/\ell}[\tilde{K} \otimes_\ell \phi]} \ell \otimes H^{\#} \xrightarrow{\ell \otimes \delta} \ell \otimes H.$$

3.4.1. LEMMA. *ψ is an isomorphism.*

Proof. Since the restriction

$$\psi: \tilde{K}X = P(C^{\#}) \to P(\ell \otimes H) = \tilde{U}_0 = \tilde{K}X$$

is an isomorphism (identified with the identity), ψ is injective (0.4). We view $C^{\#}$ as a subcoalgebra of $\ell \otimes H$ via ψ. Since $C^{\#}$ and $\ell \otimes H$ are ℓ-pseudohyperalgebras, we have only to prove $\xi_\ell(C^{\#}) = \xi_\ell(\ell \otimes H)$ by Theorem 2.4.

Put $\xi_\ell(C^{\#}) = (\tilde{U}_0' \supset \tilde{U}_1' \supset \tilde{U}_2' \supset \cdots)$, where $\tilde{U}_0' = \tilde{U}_0$ and $\tilde{U}_i' \subset \tilde{U}_i$. Let $x \in X$. There is a $(p^{(x)+1} - 1)$-SDP in C lying over x. By the same reason as (2.7), we conclude that

$$\tilde{K}x \subset \tilde{U}'_{(x)} \subset \tilde{U}_{(x)}.$$

Hence $P_i \oplus P_{i+1} \oplus \cdots \oplus P_{N-1} \subset \tilde{U}_i' \subset \tilde{U}_i$ for $i = 0, 1, \ldots, N-1$.

Let $\tilde{U}_\infty'$ be the set of elements in $\tilde{U}_0'$ over which there is an ∞-SDP in $C^{\#}$. The proof of Lemma 2.8 shows that

$$\mathfrak{a}_{(x)+1}x \subset \tilde{U}_\infty'$$

for each $x \in X$. Thus $\mathfrak{a}_i P_{i-1} \subset \tilde{U}_\infty'$ for $i = 1, 2, \ldots, N$.

This proves immediately that $\tilde{U}_i' = \tilde{U}_i$ for all $i \geqslant 0$. Hence $\xi_\ell(C^{\#}) = \xi_\ell(\ell \otimes H)$ and $\psi: C^{\#} \xrightarrow{\simeq} \ell \otimes H$. Q.E.D.

3.4.2. Let $\sigma: K \# H \to \mathrm{End}_F(K)$ denote the map of K/k-bialgebras identified with the inclusion $H \hookrightarrow hy_k(K/F)$ (see (1.4.2), (1.5), (1.8), and (1.9.1)). The composite $\tilde{K}$-coalgebra map

$$\Phi: \tilde{K} \otimes_\ell C \xrightarrow{\tilde{K} \otimes_\ell \phi} \ell \otimes (K \# H) \xrightarrow{\ell \otimes \sigma} \mathrm{End}_{\tilde{F}}(\tilde{K})$$

is *injective*, since so is the restriction on $\tilde{K} \otimes_\ell P(C) = \tilde{K}X$ and $\mathrm{End}_{\tilde{F}}(\tilde{K})$ is clearly a *flat* $\tilde{K}$-module (0.9.1).

The ℓ-coalgebra isomorphism

$$\psi^{-1}: \ell \otimes H \xrightarrow{\simeq} C^*$$

corresponds to a $\tilde{K}$-coalgebra map

$$\tau: \ell \otimes (K \# H) \to \tilde{K} \otimes_\ell C.$$

LEMMA. *The composite*

$$\ell \otimes (K \# H) \xrightarrow{\tau} \tilde{K} \otimes_\ell C \xrightarrow{\Phi} \mathrm{End}_{\tilde{F}}(\tilde{K})$$

equals $\ell \otimes \sigma$.

Proof. The ℓ-coalgebra map corresponding to $\Phi \circ \tau$ is

$$\chi: \ell \otimes H \xrightarrow{\psi^{-1}} C^* \xrightarrow{\Pi_{\tilde{K}/\ell}\Phi} \prod_{\tilde{K}/\ell} \mathrm{End}_{\tilde{F}}(\tilde{K}) = M_\ell(\tilde{K}/\tilde{F}),$$

where $\prod_{\tilde{K}/\ell} \Phi$ factors as

$$\prod_{\tilde{K}/\ell} \Phi: C^* \xrightarrow{\Pi_{\tilde{K}/\ell}[\tilde{K} \otimes_\ell \phi]} \ell \otimes H^* \xrightarrow{\ell \otimes \delta} \ell \otimes M_k(K/F) = M_\ell(\tilde{K}/\tilde{F}),$$

which equals

$$C^* \xrightarrow{\psi} \ell \otimes H \subset \ell \otimes M_k(K/F) = M_\ell(\tilde{K}/\tilde{F}).$$

Hence the ℓ-coalgebra map χ is the same as the inclusion. This means that $\Phi \circ \tau = \ell \otimes \sigma$.

3.4.3. Since $\sigma: K \# H \to \mathrm{End}_F(K)$ is surjective by (1.6.3), it follows from the above lemma that

$$\Phi: \tilde{K} \otimes_\ell C \to \mathrm{End}_{\tilde{F}}(\tilde{K})$$

(which is injective) is surjective. Hence Φ is an isomorphism. Therefore

$$\prod_{\tilde{K}/\ell} \Phi: C^* \xrightarrow{\simeq} hy_\ell(\tilde{K}/\tilde{F}) = \ell \otimes hy_k(K/F),$$

where note that $hy_\ell(\tilde{K}/\tilde{F})$ is the irreducible component containing 1 of $M_\ell(\tilde{K}/\tilde{F}) = \prod_{\tilde{K}/\ell} \mathrm{End}_{\tilde{F}}(\tilde{K})$. Since the above map is the composite

$$C^* \xrightarrow{\Pi_{\tilde{K}/\ell}[\tilde{K} \otimes_\ell \phi]} (\ell \otimes H)^* = \ell \otimes H^* \xrightarrow{\ell \otimes \delta} \ell \otimes hy_k(K/F),$$

it follows that $\delta: H^* \to hy_k(K/F)$ is *surjective*.

This proves Theorem 3.1.

4. The Galois Subbialgebras $H_k(K/F)$

Suppose k is of characteristic $p > 0$.

Let C be a cocommutative k-coalgebra. Then

$$C_{\mathrm{pt}} \underset{\mathrm{def}}{=} \bigoplus_{g \in G(C)} C^g$$

is the unique maximal *pointed* (0.3) subcoalgebra of C by [7, 8.0.7]. We call C_{pt} *the pointed part* of C.

If $u: C \to D$ is a map of cocommutative k-coalgebras, then $u: C_{\mathrm{pt}} \to D_{\mathrm{pt}}$ clearly. Any subcoalgebra of a pointed coalgebra is pointed too.

Let H be a cocommutative k-bialgebra. Then $G(H)$ is a multiplicative submonoid of H and H_{pt} is a subbialgebra of H [7, 8.1.1].

When $G(H)$ is a *group*, then $G(H)$ normalizes H^1 in the sense that

$$gH^1g^{-1} = H^1, \qquad \forall g \in G(H)$$

and we have an isomorphism of k-algebras

$$H^1 \# k[G(H)] \xrightarrow{\simeq} H_{\mathrm{pt}}, \qquad a \# g \mid\to ag,$$

[7, 8.1.5] where $k[G(H)]$ is the k-group algebra of $G(H)$.

Let K be an extension field of k. We put

$$H_k(K) = M_k(K)_{\mathrm{pt}}$$

the pointed part of the cocommutative k-bialgebra $M_k(K)$ (0.7) and

$$H_k(K/F) = M_k(K/F)_{\mathrm{pt}} = H_k(K) \cap M_k(K/F)$$

for all intermediate field $K \supset F \supset k$.

By the universality for $M_k(K/F)$, we can identify the monoid $G(H_k(K/F))$ with the monoid of F-algebra endomorphisms of K. In particular if $[K:F] < \infty$, then $G(H_k(K/F))$ is a group and we have

$$H_k(K/F) \simeq hy_k(K/F) \# k[\mathrm{Aut}_F(K)].$$

If H is a subbialgebra of $H_k(K)$, then

$$K^H = \{\lambda \in K \mid a[\lambda] = \epsilon(a)\lambda, \forall a \in H\}$$

is an intermediate field between K and k (0.7). Recall that $H = H_k(K/F)$ is the unique maximal subbialgebra of $H_k(K)$ such that $F \subset K^H$.

Consider the Galois correspondence between the sets of intermediate fields $K \supset F \supset k$ and of subbialgebras H of $H_k(K)$:

$$F \mapsto H_k(K/F) \qquad \text{and} \qquad K^H \leftarrow\!\shortmid H.$$

Sweedler proves the following:

4.1. THEOREM. [6, Theorem 2.4] *Let $K \supset F \supset k$ be fields with $[K : F] < \infty$. Then $F = K^H$ for some subbialgebra $H \subset H_k(K)$ if and only if*

(1) *K is normal over F,*

(2) *F and kK^{p^n} are linearly disjoint over $F \cap kK^{p^n}$ for all n.*

In this section we characterize the subbialgebras $H_k(K/F)$ for $[K : F] < \infty$.

For each pointed cocommutative k-bialgebra H with a measuring representation $\rho: H \to \mathrm{End}_k(K)$, let

$$H^{\#} = \left[\prod_{K/k} (K \# H)\right]_{\mathrm{pt}}$$

denote the pointed part of the k-bialgebra $\prod_{K/k} (K \# H)$ (1.9).

Since $G(H^{\#}) = G(K \# H) = G(H)$ (because the K-coalgebra $K \# H$ is pointed), it follows that the adjunction

$$\iota: H \to H^{\#}$$

induces an isomorphism $\iota: G(H) \xrightarrow{\simeq} G(H^{\#})$. Hence if $G(H)$ is a group, so is $G(H^{\#})$.

If H is *irreducible* (i.e., H is a *k-hyperalgebra*), then so is $H^{\#}$, since $G(H^{\#}) = \{1\}$. Hence the notation $H^{\#}$ here is compatible with the convention in (1.9.1).

We have already used, in (3.3.7), the following:

4.2. PROPOSITION. [7, 10.2.1] *If $H \subset hy_k(K)$ is a subbialgebra and K is algebraic over $F = K^H$, then K/F is purely inseparable.*

When K/F is algebraic, let $K \supset F_{\mathrm{sep}} \supset F$ be the separable closure of F in K.

4.3. COROLLARY. *If K/F is algebraic, then $hy_k(K/F) = H_k(K/F_{\mathrm{sep}})$.*

Proof. The inclusion $hy_k(K/F) \subset H_k(K/F_{\mathrm{sep}})$ follows from above. Since $\mathrm{Aut}_{F_{\mathrm{sep}}}(K) = \{1\}$, $H_k(K/F_{\mathrm{sep}}) \subset hy_k(K/F)$. Q.E.D.

If H is a subbialgebra of $H_k(K)$, the inclusion $H \hookrightarrow H_k(K)$ induces a map of k-bialgebras

$$\delta: \prod_{K/k} (K \# H) \to M_k(K).$$

Taking the pointed parts, we obtain

$$\delta: H^{\#} \to H_k(K).$$

4.4. THEOREM. *Let H be a subbialgebra of $H_k(K)$ and $\sigma: K \# H \to \mathrm{End}_k(K)$ the associated measuring representation* (1.5). *Then $H = H_k(K/F)$ for some subfield $K \supset F \supset k$ with $[K:F] < \infty$ if and only if*

(1) *$\sigma(K \# H)$ is a finite-dimensional left K-vector space,*

(2) $\delta(H^{\#}) \subset H$.

Proof. The "only if" part is clear. By (1.6.3) the condition (1) implies that $[K:K^H] < \infty$. Put $F = K^H$. Suppose $[K:F] < \infty$ and $\delta(H^{\#}) \subset H$. Let $L = K^{(H^1)}$. Then $[K:L] < \infty$ and $\delta((H^1)^{\#}) \subset H^1$. Hence $H^1 = hy_k(K/L)$ by Theorem 3.1.

Since $G = G(H)$ is a submonoid of the *finite* group $G(H_k(K/F)) = \mathrm{Aut}_F(K)$, G is also a group. Since the group G normalizes H^1, it normalizes the invariant field L. The group homomorphism

$$G \to \mathrm{Aut}_F(L)$$

induced from $H \hookrightarrow H_k(K/F)$ is *surjective*, since $L^G = F$. In particular the finite extension L/F is *galois*. Since K/L is purely inseparable by (4.2), it follows that $L = F_{\mathrm{sep}}$. Hence $H^1 = hy_k(K/L) = hy_k(K/F)$.

Further, since K/F is *normal* by (4.1), we have

$$\mathrm{Aut}_F(K) \xrightarrow{\simeq} \mathrm{Aut}_F(F_{\mathrm{sep}}).$$

Hence $G \xrightarrow{\simeq} \mathrm{Aut}_F(K) = G(H_k(K/F))$. Therefore

$$H = H^1 \# k[G] \xrightarrow{\simeq} hy_k(K/F) \# k[G(H_k(K/F))] \simeq H_k(K/F). \qquad \text{Q.E.D.}$$

4.5. COROLLARY. *There is a bijective Galois correspondence between the set of intermediate fields $K \supset F \supset k$ such that K/F is finite normal and F and kK^{p^n} are linearly disjoint for all n and the set of subbialgebras $H \subset H_k(K)$ such that $[\sigma(K \# H):K] < \infty$ and $\delta(H^{\#}) \subset H$ via $F \mapsto H_k(K/F)$ and $K^H \leftarrow\!\shortmid H$.*

5. A COUNTER EXAMPLE

This section shows that Theorem 3.1 does not hold if the assumption $[K:F] < \infty$ is dropped.

Let K/k be an extension of fields of characteristic $p > 0$. Let L be a k-hyperalgebra and $\alpha: L \to hy_k(K)$ a hyperalgebra map. Suppose that the associated hyperalgebra map (1.9.1) $\delta: L^{\#} \to hy_k(K)$ is *injective*. Then the image $H = \delta(L^{\#})$ satisfies the condition $\delta(H^{\#}) \subset H$ in (3.1).

Indeed the isomorphism $\delta^{-1}: H \xrightarrow{\simeq} L^{\#}$ in the category $\mathfrak{Q}$ (1.7) determines

a K/k-bialgebra map $u: K \# H \to K \# L$ by (1.7.6). Then u induces an Ω-map $\prod_{K/k} u: H^{\#} \to L^{\#}$, or equivalently the composite

$$H^{\#} \xrightarrow{\Pi_{K/k} u} L^{\#} \xrightarrow{\delta} hy_k(K)$$

is associated with the inclusion $H \subset hy_k(K)$ in the sense of (1.9.1). Hence $\delta(H^{\#}) \subset H$.

Note that $\delta: L^{\#} \to hy_k(K)$ is injective if and only if the Lie algebra map $\alpha: P(L) \to \mathrm{Der}_k(K)$ induces an injection $K \otimes P(L) \subset \mathrm{Der}_k(K)$ (1.9.2).

Suppose $k = K^L = K^H$ and K/k is *finitely generated*. For each $n \geqslant 0$, K is finite purely inseparable over kK^{p^n} and there is a subhyperalgebra $M \subset hy_k(K)$ with $kK^{p^n} = K^M$ by Theorem 4.1.

Hence in order to show $H \neq hy_k(K)$, it is enough to show that there is an integer $n > 0$ such that there is no subhyperalgebra $M \subset H$ with $K^M = kK^{p^n}$.

Put $L = B_k = kb_0 + kb_1 + kb_2 + \cdots$ (0.4). This is a hyperalgebra by $1 = b_0$ and $b_i b_j = \binom{i+j}{i} b_{i+j}$. Giving a hyperalgebra map $\alpha: L \to hy_k(K)$ is equivalent to giving a k-algebra map

$$\chi: K \to K[[t]] \qquad \text{(the power series } K\text{-algebra)}$$

such that $\phi_0 \circ \chi = \phi_1 \circ \chi$ and $\epsilon \circ \chi = I$, where

$$\phi_0 : K[[t]] \to K[[t, u]], \qquad \sum_i \lambda_i t^i \mapsto \sum_i \chi(\lambda_i) u^i,$$

$$\phi_1 : K[[t]] \to K[[t, u]], \qquad \sum_i \lambda_i t^i \mapsto \sum_i \lambda_i (t + u)^i,$$

$$\epsilon : K[[t]] \to K, \qquad \sum_i \lambda_i t^i \mapsto \lambda_0 .$$

The associated map $\delta: L^{\#} \to hy_k(K)$ is injective if and only if $\alpha(b_1) \neq 0$ if and only if the composite $K \xrightarrow{\chi} K[[t]] \to K[t]/(t^2)$ is nontrivial.

Let $k[\mathbb{F}]$ be the noncommutative polynomial ring with $\mathbb{F}\lambda = \lambda^p \mathbb{F}$, $\lambda \in K$. All commutative k-algebra R is a left $k[\mathbb{F}]$-module by $\mathbb{F}a = a^p$, $a \in R$.

In the power series k-algebra $k[[t]]$ let $P(k[[t]])$ denote the subspace of *p-power* power series $\lambda_0 t + \lambda_1 t^p + \lambda_2 t^{p^2} + \cdots + \lambda_n t^{p^n} + \cdots$, $\lambda_i \in k$. This is a $k[\mathbb{F}]$-subspace and hence a commutative p-Lie subalgebra. The induced algebra map $U^{[p]}(P(k[[t]])) \to k[[t]]$, where $U^{[p]}(X)$ denotes the universal enveloping algebra of the p-Lie algebra X, is *injective*.

In particular if S is a finite subset of $P(k[[t]])$ linearly independent over $k[\mathbb{F}]$, by which we mean $\alpha_q = 0$, $\forall q \in S$, when $\sum_q \alpha_q q = 0$ with $\alpha_q \in k[\mathbb{F}]$, then S is *algebraically independent* over k.

Fix an integer $a > 1$ and put

$$u = t^p + t^{p^a} + t^{p^{a^2}} + \cdots + t^{p^{a^n}} + \cdots.$$

Then $\{t, u\}$ are linearly independent over $k[\mathbb{F}]$ and hence algebraically independent over k.

Let $K = k(x, y)$ be purely transcendental over k with the indeterminates x and y. Define a k-algebra map $\chi: K \to K[[t]]$ by

$$\chi(x) = x + t \qquad \text{and} \qquad \chi(y) = y + u.$$

Since $t, u \in P(k[[t]])$, χ satisfies the conditions $\phi_0 \circ \chi = \phi_1 \circ \chi$ and $\epsilon \circ \chi = I$ and determines a hyperalgebra map $\alpha: L = B_k \to hy_k(K)$.

The K-algebra map

$$\bar{\chi}: K \otimes K \to K[[t]], \qquad \lambda \otimes \mu \mapsto \lambda \cdot \chi(\mu)$$

is *injective*, since $\{t, u\}$ are algebraically independent over k. It follows that $k = K^L$.

The associated hyperalgebra map $\delta: L^* \to hy_k(K)$ is *injective*, since $\alpha(b_1) \neq 0$. We put $H = \delta(L^*)$ and show $H \neq hy_k(K)$.

For each integer $n > 0$ put

$$K_n = k\left(x^{p^n}, y^{p^n}, -y + \sum_{0<a^i<n} x^{p^{a^i}}\right),$$

$$L_n = kb_0 + kb_1 + \cdots + kb_{p^n-1},$$

where L_n is a subhyperalgebra of L.

It is clear that $K_n \subset K^{L_n}$.

The canonical measuring representation (1.4.2) $\sigma: K \# L \to \mathrm{End}_k(K)$ induces maps of K/k-bialgebras

$$\sigma: K \# L_n \to \mathrm{End}_{K_n}(K).$$

Hence the image $\sigma(K \# L)$ is contained in

$$\mathscr{H} = \bigcup_{n=1}^{\infty} \mathrm{End}_{K_n}(K),$$

which is a K/k-bialgebra. The composite map of K/k-bialgebras $K \# H \xrightarrow{u} K \# L \xrightarrow{\sigma} \mathscr{H}$ where u is defined before, corresponds to the inclusion $H \hookrightarrow hy_k(K)$.

Note that the sequence of subfields $K \supset K_1 \supset K_2 \supset \cdots$ satisfies

$$K_n = K_{n+1}K^{p^n}, \qquad \forall n \geqslant 0,$$

where we put $K_0 = K$. Hence for $r \geqslant n \geqslant 0$, $K_n = K_r K^{p^n}$. Therefore $\mathrm{End}_{K_r}(K) \cap \mathrm{End}_{kK^{p^n}}(K) = \mathrm{End}_{K_n}(K)$. This proves

$$\mathscr{H} \cap \mathrm{End}_{kK^{p^n}}(K) = \mathrm{End}_{K_n}(K).$$

Now put

$$H_n = H \cap hy_k(K/kK^{p^n}).$$

Since the inclusion $H_n \subset\!\!\rightarrow hy_k(K/kK^{p^n})$ corresponds to the K/k-bialgebra map

$$\sigma \circ u\colon K \# H_n \to \mathscr{H} \cap \mathrm{End}_{kK^{p^n}}(K) = \mathrm{End}_{K_n}(K)$$

it follows that $K_n \subset K^{H_n}$. Since $K_n \neq kK^{p^n}$, it follows that $H_n \neq hy_k(K/kK^{p^n})$ for all $n > 0$. Therefore $H \neq hy_k(K)$.

APPENDIX: Translation into the Language of the Group Schemers

Let us start with the following simple remark due to S. Chase [2, Sect. 9]: Let Γ be a monoid and X a right Γ-set with the action $X \times \Gamma \to X$, $(x, \gamma) \mapsto x\gamma$. The set Γ^X of all maps from X into Γ is a monoid if we define product by

$$(uv)(x) = u(x)\, v(xu(x))$$

for $x \in X$ and $u, v \in \Gamma^X$. The unit of Γ^X is $e\colon X \to \Gamma$, where $e(x) = 1$ for all $x \in X$. The set X^X of endomorphisms of X is a monoid under composition and the map $\delta\colon \Gamma^X \to X^X$ defined by

$$\delta(u)(x) = xu(x)$$

for $x \in X$ and $u \in \Gamma^X$, is an antihomomorphism of monoids. Hence X becomes a right Γ^X-set. The canonical map $\iota\colon \Gamma \to \Gamma^X$ defined by $\iota(\gamma)(x) = \gamma$ for $\gamma \in \Gamma$ and $x \in X$ is a monoid map and the Γ-action on X pulled back along ι coincides with the original action.

This observation has some generalization.

First Generalization. Let A be a category with *finite products*. Let Γ be a *monoid object* in A and X a *right Γ-object* in A. If Y is an object of A, then $\mathsf{A}(Y, \Gamma)$ is a usual monoid and $\mathsf{A}(Y, X)$ is a right $\mathsf{A}(Y, \Gamma)$-set. Hence $\mathsf{A}(Y, \Gamma)^{\mathsf{A}(Y,X)}$ is a monoid by the above remark for all $Y \in \mathsf{A}$. By Yoneda's Lemma, the set $\mathsf{A}(X, \Gamma)$ can be viewed as a subset of $\prod_{Y \in \mathsf{A}} \mathsf{A}(Y, \Gamma)^{\mathsf{A}(Y,X)}$. It is a submonoid of the direct product of monoids. Since each $\mathsf{A}(Y, X)$ is a right $\mathsf{A}(Y, \Gamma)^{\mathsf{A}(Y,X)}$-set, it is a right $\mathsf{A}(X, \Gamma)$-set through the projection: $\mathsf{A}(X, \Gamma) \to \mathsf{A}(Y, \Gamma)^{\mathsf{A}(Y,X)}$. Since this $\mathsf{A}(X, \Gamma)$-operation on $\mathsf{A}(Y, X)$ is natural with respect to $Y \in \mathsf{A}$, a canonical antihomomorphism of monoids

$$\delta\colon \mathsf{A}(X, \Gamma) \to \mathsf{A}(X, X)$$

follows.

Second Generalization. Let A be a category with finite products and Γ, X be as above. Suppose in addition the existence of the "internal hom" functor $[-, -]: \mathsf{A}^{\mathrm{op}} \times \mathsf{A} \to \mathsf{A}$ characterized by

$$\mathsf{A}(Y \times Z, W) \simeq \mathsf{A}(Y, [Z, W])$$

naturally for $Y, Z, W \in \mathsf{A}$. For each object $Y \in \mathsf{A}$, $Y \times X$ is a right Γ-object by $Y \times \phi: (Y \times X) \times \Gamma \to Y \times X$ where $\phi: X \times \Gamma \to X$ denotes the Γ-action on X. Hence $\mathsf{A}(Y \times X, \Gamma)$ is a monoid by the above generalized observation. This means that $\mathsf{A}(Y, [X, \Gamma])$ has a natural monoid structure for all $Y \in \mathsf{A}$. Hence by definition $[X, \Gamma]$ is a monoid object in A.

For two objects $Y, W \in \mathsf{A}$, let

$$\zeta: [Y, Z] \times Y \to Z$$

correspond with the identity of $[Y, Z]$. For $Y, Z, W \in \mathsf{A}$, the *composition* map (in A)

$$c: [Y, Z] \times [W, Y] \to [W, Z]$$

corresponds to the composite

$$[Y, Z] \times [W, Y] \times W \xrightarrow{[Y,Z]\times\zeta} [Y, Z] \times Y \xrightarrow{\zeta} Z.$$

Then the object $[X, X]$ is a monoid object in A "under composition."

Let $\mathsf{A}_{/Y}$ denote the category of "objects in A over Y" for each $Y \in \mathsf{A}$. $Y \times X$ is an object in $\mathsf{A}_{/Y}$ with the projection $\mathrm{pr}_1: Y \times X \to Y$ as the structure map. The composite

$$\mathsf{A}_{/Y}(Y \times X, Y \times X) \simeq \mathsf{A}(Y \times X, X) \simeq \mathsf{A}(Y, [X, X])$$

is an isomorphism of *monoids*.

We have a natural antihomomorphism of monoids

$$\delta: \mathsf{A}(Y \times X, \Gamma) \to \mathsf{A}(Y \times X, Y \times X),$$

whose image is seen to be contained in the submonoid $\mathsf{A}_{/Y}(Y \times X, Y \times X)$. The composite of monoid homomorphisms

$$\mathsf{A}(Y, [X, \Gamma]) \simeq \mathsf{A}(Y \times X, \Gamma) \xrightarrow{\delta} \mathsf{A}_{/Y}(Y \times X, Y \times X)^{\mathrm{op}} \simeq \mathsf{A}(Y, [X, X])^{\mathrm{op}}$$

is clearly natural with respect to $Y \in \mathsf{A}$ and hence, by Yoneda's Lemma, this gives rise to an antihomomorphism of monoid objects in A:

$$\delta: [X, \Gamma] \to [X, X]$$

or equivalently the monoid object $[X, \Gamma]$ operates on X on the *right* via the composite

$$X \times [X, \Gamma] \xrightarrow{\text{twist}} [X, \Gamma] \times X \xrightarrow{d} X,$$

where d corresponds to δ. The canonical map

$$\iota: \Gamma \to [X, \Gamma]$$

which is associated with the projection: $\Gamma \times X \to \Gamma$, is a map of monoid objects in A commuting with the operations on X.

We apply this second generalization to the category of *k-functors*.

Fix a commutative ring k. M_k (resp. E) denotes the category of small commutative k-algebras (resp. sets). For "smallness" see [3, Conventions]. A *k-functor* is a functor from M_k to E. The category of k-functors is denoted by $\mathsf{M}_k\mathsf{E}$.

The category $\mathsf{M}_k\mathsf{E}$ has direct products and the internal hom functor $\mathfrak{Hom}_k(-, -): (\mathsf{M}_k\mathsf{E})^{\mathrm{op}} \times \mathsf{M}_k\mathsf{E} \to \mathsf{M}_k\mathsf{E}$ [3, I, Sect. 2, 7.1], where $\mathfrak{Hom}_k(\mathfrak{Y}, \mathfrak{Z})$ is defined by

$$\mathfrak{Hom}_k(\mathfrak{Y}, \mathfrak{Z})(R) = \mathsf{M}_k\mathsf{E}(\mathfrak{Sp}(R) \times \mathfrak{Y}, \mathfrak{Z})$$

for all $R \in \mathsf{M}_k$ and $\mathfrak{Y}, \mathfrak{Z} \in \mathsf{M}_k\mathsf{E}$, where

$$\mathfrak{Sp}(R): \mathsf{M}_k \to \mathsf{E}, \qquad T \mapsto \mathsf{M}_k(R, T)$$

denotes the *affine* k-functor determined by R.

The monoid objects in $\mathsf{M}_k\mathsf{E}$ are the same as the functors from M_k to the category of monoids. They are called the *k-monoid functors* [3, p. 140].

Hence if a k-monoid functor $\mathfrak{G}$ operates on a k-functor $\mathfrak{X}$ on the right [3, p. 160], then $\mathfrak{Hom}_k(\mathfrak{X}, \mathfrak{G})$ has a canonical monoid structure and there is a canonical antihomomorphism of monoid functors

$$\delta: \mathfrak{Hom}_k(\mathfrak{X}, \mathfrak{G}) \to \mathfrak{Hom}_k(\mathfrak{X}, \mathfrak{X})$$

where the right-hand side is a k-monoid functor under composition. The canonical morphism $\iota: \mathfrak{G} \to \mathfrak{Hom}_k(\mathfrak{X}, \mathfrak{G})$ is a homomorphism of monoid functors and the composition $\delta \circ \iota$ corresponds to the original operation.

Consider the particular case when $\mathfrak{X}$ is *affine*. Let $\mathfrak{X} = \mathfrak{Sp}(K)$ with $K \in \mathsf{M}_k$. The k-monoid functor $\mathfrak{Hom}_k(\mathfrak{X}, \mathfrak{X})$ is then antiisomorphic with the k-monoid functor $\mathfrak{End}(K)$ where $\mathfrak{End}(K)(R)$ is the monoid of all R-algebra endomorphisms of $K \otimes R$ for each $R \in \mathsf{M}_k$ [3, II, Sect. 1, 2.6].

Since we have $\mathfrak{Hom}_k(\mathfrak{X}, \mathfrak{G})(R) = \mathsf{M}_k\mathsf{E}(\mathfrak{Sp}(R) \times \mathfrak{Sp}(K), \mathfrak{G}) \simeq \mathfrak{G}(K \otimes R)$ naturally for $R \in \mathsf{M}_k$, it follows that

$$\mathfrak{Hom}_k(\mathfrak{X}, \mathfrak{G}) \simeq \mathfrak{G}^{\#},$$

where $\mathfrak{G}^{\#} = \prod_{K/k}(K \otimes \mathfrak{G})$ is the k-functor $R \mapsto \mathfrak{G}(K \otimes R)$, $R \in \mathsf{M}_k$. Hence we can transport the monoid structure on $\mathfrak{Hom}_k(\mathfrak{X}, \mathfrak{G})$ to $\mathfrak{G}^{\#}$ by means of the canonical isomorphism. The result is as follows.

Let $\alpha: \mathfrak{G} \to \mathfrak{End}(K)$ be the map of monoid functors associated with the right $\mathfrak{G}$-operation on $\mathfrak{X} = \mathfrak{Sp}(K)$. For each $g \in \mathfrak{G}(K \otimes R)$ with $R \in \mathsf{M}_k$, put

$$\delta(g): K \otimes R \xrightarrow{i \otimes R} K \otimes K \otimes R \xrightarrow{\alpha[g]} K \otimes K \otimes R \xrightarrow{m \otimes R} K \otimes R,$$

where $i(\lambda) = \lambda \otimes 1$ and $m(\lambda \otimes \mu) = \lambda\mu$ for $\lambda, \mu \in K$. Since $\delta(g)$ is an R-algebra endomorphism of $K \otimes R$, this gives rise to a morphism of k-functors

$$\delta: \mathfrak{G}^{\#} \to \mathfrak{End}(K).$$

Further the R-algebra endomorphism $\delta(g)$ induces a monoid map

$$\mathfrak{G}(\delta(g)): \mathfrak{G}(K \otimes R) \to \mathfrak{G}(K \otimes R).$$

For each $f, g \in \mathfrak{G}(K \otimes R)$, define a product

$$f * g = f \cdot \mathfrak{G}(\delta(f))(g)$$

where the right-hand side is the product of f with $\mathfrak{G}(\delta(f))(g)$ in the monoid $\mathfrak{G}(K \otimes R)$. The product $*$ is associative with the same unit as $\mathfrak{G}(K \otimes R)$ and makes $\mathfrak{G}^{\#}$ into a k-monoid functor. The morphism $\delta: \mathfrak{G}^{\#} \to \mathfrak{End}(K)$ is a homomorphism of k-monoid functors.

The canonical morphism $\iota: \mathfrak{G} \to \mathfrak{G}^{\#}$, where $\iota(R): \mathfrak{G}(R) \to \mathfrak{G}^{\#}(R) = \mathfrak{G}(K \otimes R)$ are induced from the canonical R-algebra maps $R = k \otimes R \to K \otimes R$, is a homomorphism of monoid functors and we have $\alpha = \delta \circ \iota$.

It is easy to show that the canonical isomorphism $\mathfrak{Hom}_k(\mathfrak{X}, \mathfrak{G}) \simeq \mathfrak{G}^{\#}$ is an isomorphism of monoid functors and that the right operation of $\mathfrak{Hom}_k(\mathfrak{X}, \mathfrak{G})$ on $\mathfrak{X}$ corresponds to $\delta: \mathfrak{G}^{\#} \to \mathfrak{End}(K)$. The canonical map $\iota: \mathfrak{G} \to \mathfrak{Hom}_k(\mathfrak{X}, \mathfrak{G})$ corresponds with $\iota: \mathfrak{G} \to \mathfrak{G}^{\#}$.

In order to combine the above arguments with the process of making $(H^{\#}, \delta)$ in Sect. 1.9, we shall need the theory of *tangent coalgebras* [8].

In the following let k be a field and K a commutative k-algebra. Let M_k^f be the category of commutative k-algebras R which are finite dimensional as k-vector spaces. A functor $X: \mathsf{M}_k^f \to \mathsf{E}$ is a *k-formal scheme* if it preserves the finite $\varinjlim$, that is, if it preserves all the finite products and the equalizer diagrams. For each $C \in \mathsf{W}_k$, the functor

$$\mathrm{Sp}^* C: \mathsf{M}_k^f \to \mathsf{E}, \qquad R \mapsto \mathsf{W}_k({}^tR, C)$$

is a k-formal scheme and the functor

$$\mathrm{Sp}^*\colon C \mapsto \mathrm{Sp}^* C$$

gives an equivalence between W_k and the category of k-formal schemes.

A k-functor $\mathfrak{X}$ is said to *have the underlying coalgebra* $T(\mathfrak{X})$ if the restriction $\mathfrak{X} \mid \mathsf{M}_k{}^f$ is a k-formal scheme with $\mathfrak{X} \mid \mathsf{M}_k{}^f \simeq \mathrm{Sp}^*(T(\mathfrak{X}))$, or equivalently if

$$\mathfrak{X}(R) \simeq \mathsf{W}_k({}^tR, T(\mathfrak{X})) \qquad (\dagger)$$

for all $R \in \mathsf{M}_k{}^f$ naturally.

All k-schemes have the underlying coalgebra [8, 2.1.6].

If $\mathfrak{X}$ is a k-monoid functor having the underlying coalgebra $T(\mathfrak{X})$, then there is a unique algebra structure on $T(\mathfrak{X})$ which makes it into a bialgebra and all the isomorphisms (†) into monoid isomorphisms, since the monoid objects in W_k are the same as the cocommutative bialgebras. This is called *the underlying bialgebra* of $\mathfrak{X}$.

The k-monoid functor $\mathfrak{End}(K)$ has $M_k(K)$ as the underlying bialgebra [8, 3.2.7].

For each k-functor $\mathfrak{X}$ (resp. K-functor $\mathfrak{Y}$), the K-functor $K \otimes \mathfrak{X}$ (resp. the k-functor $\prod_{K/k} \mathfrak{Y}$) is defined by

$$(K \otimes \mathfrak{X})(S) = \mathfrak{X}(S) \qquad \left(\text{resp. } \left(\prod_{K/k} \mathfrak{Y}\right)(R) = \mathfrak{Y}(K \otimes R)\right)$$

for all $S \in \mathsf{M}_K$ (resp. $R \in \mathsf{M}_k$).

Suppose $\mathfrak{X}$ is a k-functor such that the k-functors $\mathfrak{X}$ and $\prod_{K/k}(K \otimes \mathfrak{X})$ both have the underlying coalgebras. This happens if the k-functor $\mathfrak{X}$ itself commutes with the finite $\varinjlim$, since the functor $\mathsf{M}_k \to \mathsf{M}_k$, $R \mapsto K \otimes R$ commutes with the finite $\varinjlim$. $\mathfrak{End}(K)$ is an example of such k-functors. We can define a natural homomorphism of k-coalgebras

$$\xi\colon \prod_{K/k} (K \otimes T(\mathfrak{X})) \to T\left(\prod_{K/k} (K \otimes \mathfrak{X})\right)$$

as follows (cf. [8, 2.2.8]): Let $u\colon C \to \prod_{K/k}(K \otimes T(\mathfrak{X}))$ be a W_k-map where C is finite dimensional over k. We can identify u as a W_K-map $U\colon K \otimes C \to K \otimes T(\mathfrak{X})$. There is a finite dimensional subcoalgebra D of $T(\mathfrak{X})$ such that $K \otimes D$ contains $\mathrm{Im}(U)$. The inclusion $D \subset T(\mathfrak{X})$ corresponds to an element $i \in \mathfrak{X}({}^tD)$. The composition

$${}^tD \xrightarrow{\text{cano}} K \otimes {}^tD \xrightarrow{{}^tU} K \otimes {}^tC$$

sends i to some element $j \in \mathfrak{X}(K \otimes {}^tC) = (\prod_{K/k}(K \otimes \mathfrak{X}))({}^tC)$. View j as a W_k-map $J\colon C \to T(\prod_{K/k}(K \otimes \mathfrak{X}))$ which does not depend on the choice

of D. Since the formation $u \mapsto J$ is clearly natural, there is a unique W_k-map ξ such that $J = \xi \circ u$ for all (C, u) with $C \in \mathsf{W}_k$ finite dimensional.

Let $\mathfrak{G}$ be a k-monoid functor and $\alpha: \mathfrak{G} \to \mathfrak{End}(K)$ a homomorphism of k-monoid functors. Suppose $\mathfrak{G}$ and $\prod_{K/k}(K \otimes \mathfrak{G})$ have the underlying coalgebras. The composite

$$\alpha: T(\mathfrak{G}) \xrightarrow{T(\alpha)} T(\mathfrak{End}(K)) = M_k(K)$$

is a homomorphism of cocommutative k-bialgebras. We have a k-monoid functor $\mathfrak{G}^{\#} = \prod_{K/k}(K \otimes \mathfrak{G})$ and a homomorphism of k-monoid functors

$$\delta: \mathfrak{G}^{\#} \to \mathfrak{End}(K)$$

by the above observation. On the other hand we have a cocommutative k-bialgebra $\prod_{K/k}(K \# T(\mathfrak{G}))$ and a homomorphism of bialgebras

$$\delta: \prod_{K/k}(K \# T(\mathfrak{G})) \to M_k(K)$$

by Section 1.9. The reader can prove that the diagram

$$\begin{array}{ccccc} & & \prod\limits_{K/k}(K \# T(\mathfrak{G})) & \xrightarrow{\delta} & M_k(K) \\ & \overset{\iota}{\nearrow} & \downarrow \xi & & \| \\ T(\mathfrak{G}) & \xrightarrow{T(\iota)} & T(\mathfrak{G}^{\#}) & \xrightarrow{T(\delta)} & T(\mathfrak{End}(K)) \end{array}$$

commutes, where the map ξ is a homomorphism of *bialgebras*.

If $\mathfrak{G}$ is a *locally algebraic k-monoid scheme* and K/k is an *algebraic* extension of fields, then the homomorphism ξ is an isomorphism by [8, 2.2.8]. This occurs when K/k is a finite extension and $\mathfrak{G} = \mathfrak{End}(K)$.

References

1. H. Bass, "Algebraic K-Theory," Benjamin, New York, 1968.
2. S. Chase, Infinitesimal group scheme actions on finite field extensions, preprint.
3. M. Demazure and P. Gabriel, "Groupes algébriques," tome I, North-Holland, Amsterdam, 1970.
4. R. Heyneman and M. Sweedler, Affine Hopf algebras, I, II, *J. Algebra* **13** (1969), 192–241; **16** (1970), 271–297.
5. M. Sweedler, Hopf algebras with one group-like element, *Trans. Amer. Math. Soc.* **127** (1967), 515–526.
6. M. Sweedler, The Hopf algebra of an algebra applied to field theory, *J. Algebra* **8** (1968), 262–276.
7. M. Sweedler, "Hopf Algebras," Benjamin, New York, 1969.

8. M. TAKEUCHI, Tangent coalgebras and hyperalgebras, I, *Jap. J. Math.* **42** (1974), 1–143.
9. D. WINTER, Normal field extensions K/k and K/k-bialgebras, *Bull. Amer. Math. Soc.* **80** (1974), 506–512.
10. M. BARR, Coalgebras over a commutative ring, *J. Algebra* **32** (1974), 600–610.
11. M. SWEEDLER, Groups of simple algebras, *Inst. Hautes Études Sci. Publ. Math.* **44** (1975), 79–189.